IBM System Storage: Implementing an IBM SAN

Discover the latest additions to the IBM SAN family

Enhance your skills while using an easy-to-follow format

Grow with the new technology

Jon Tate
Kerry Edwards
Michael Engelbrecht
Simon Richardson

Redbooks

ibm.com/redbooks

International Technical Support Organization

IBM System Storage: Implementing an IBM SAN

May 2007

SG24-6116-06

Note: Before using this information and the product it supports, read the information in "Notices" on page xi.

Seventh Edition (May 2007)

This edition applies to the hardware and firmware that was available to IBM® at the time of writing.

© Copyright International Business Machines Corporation 1999-2007. All rights reserved.
Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices xi
Trademarks xii

Preface xiii
The team that wrote this book xiii
Become a published author xvi
Comments welcome xvi

Summary of changes xvii
May 2007, Seventh Edition xvii

Chapter 1. Implementing a SAN with the b-type family 1
1.1 Product introduction 2
  1.1.1 Hardware 2
  1.1.2 Fabric Operating System 7
  1.1.3 Management tools 7
  1.1.4 Licensing 7
  1.1.5 Security 8
  1.1.6 Support 8
1.2 The hardware 8
  1.2.1 Generic features 9
  1.2.2 New features 13
1.3 Operating system 15
  1.3.1 Fabric Operating System 16
1.4 Management tools 28
  1.4.1 WebTools 28
  1.4.2 Fabric Watch 28
  1.4.3 SNMP 31
  1.4.4 Fabric Manager 32
1.5 Licensing 36
  1.5.1 Ports on Demand 36
  1.5.2 Extended Fabric 37
  1.5.3 Performance Monitoring 37
  1.5.4 ISL Trunking 38
1.6 Security 38
  1.6.1 Advanced Security / Secure Fabric OS 38
1.7 Implementation 41
  1.7.1 Initial setup 41
  1.7.2 The command line interface 44

© Copyright IBM Corp. 1999-2007. All rights reserved.

1.7.3 Connecting to the switch 52
1.7.4 SAN16B Quick Setup with EZSwitchSetup v2.1.0 61
1.8 WebTools walk-through. 86
1.8.1 Fabric Events icon. 89
1.8.2 Topology icon 91
1.8.3 Name Server icon 92
1.8.4 Zoning icon 96
1.8.5 Main view 97
1.8.6 Port information. 99
1.8.7 Status button 104
1.8.8 High Availability button 108
1.8.9 Power button 113
1.8.10 Fan button 113
1.8.11 Temp button 114
1.8.12 Admin button 115
1.8.13 Telnet button 150
1.8.14 Beaconing button 151
1.8.15 Performance Monitor button 152
1.8.16 Advanced Performance Monitoring. 163
1.8.17 Performance Monitoring with Telnet commands. 163
1.8.18 Performance Monitoring with WebTools 164
1.8.19 Using Advanced Performance Monitoring with WebTools 165
1.8.20 Using Advanced Performance Monitoring with the CLI. 172
1.8.21 Fabric Watch button 181
1.9 Fabric Manager 194
1.9.1 Fabric Manager requirements 194
1.9.2 Installing Fabric Manager 196
1.9.3 Fabric Manager Interface overview. 198
1.9.4 Launching Fabric Manager 200
1.9.5 Implementing Fabric Manager 200
1.9.6 Troubleshooting Fabric Manager 252
1.9.7 Upgrading the switch. 254
1.9.8 Advanced Security 274
1.9.9 Zoning 291
1.9.10 Implementing zoning 294
1.9.11 Multiple switch environments 310
1.9.12 FCIP/iFCP 329
1.10 Health and troubleshooting 329
1.10.1 SAN Health 329
1.10.2 Error logs. 338
1.11 FICON 340
1.11.1 FICON servers 340
1.11.2 Intermixed FICON and FCP 340

1.11.3 Cascaded FICON and CUP support 340
1.12 FICON quickstart. 343
1.13 Hardware Configuration Definition 343
1.13.1 Configure the routing policy 345
1.13.2 Disabling Dynamic Load Sharing 346
1.13.3 Configuring In-Order Delivery 347
1.13.4 Configuring Domain ID and Insistent Domain ID 349
1.14 Preparing a cascaded FICON configuration 354
1.14.1 Installing security certificates and keys. 354
1.14.2 Enabling secure mode 355
1.14.3 Configuring Switch Connection Control 357
1.14.4 Enabling FICON CUP 359
1.14.5 Configuring port connectivity. 363
1.14.6 Zoning and PDCM considerations 368
1.14.7 Displaying and configuring ports 369

Chapter 2. Implementing a SAN with the m-type family 379
2.1 Product introduction 380
2.1.1 Hardware. 380
2.1.2 Operating system 386
2.1.3 Management tools. 386
2.1.4 Licensing 387
2.1.5 Security 387
2.2 Hardware. 388
2.2.1 Features 389
2.3 Operating system 390
2.3.1 Zone types and limits 390
2.3.2 Element Manager 391
2.3.3 Preferred Path. 391
2.3.4 Full Volatility 391
2.3.5 Open Trunking 391
2.3.6 N_Port ID Virtualization. 392
2.3.7 Port fencing. 392
2.3.8 Safe zoning mode 392
2.3.9 Domain RSCNs. 393
2.3.10 Suppress RSCNs on zone set activations 393
2.3.11 Logs 393
2.3.12 Firmware upgrade. 394
2.4 Management tools. 394
2.5 Out-of-band 394
2.5.1 EFCM Basic 394
2.5.2 CLI. 399
2.5.3 SNMP 400

  - 2.5.4 SMI-S 400
  - 2.5.5 Maintenance port 400
- 2.6 In-band 401
  - 2.6.1 Open Systems Management Server (OSMS) 401
  - 2.6.2 FICON Management Server (FMS) 401
- 2.7 Security 402
- 2.8 Zoning 402
- 2.9 Role Based Access Control 402
- 2.10 SANtegrity Binding 403
  - 2.10.1 Fabric Binding 403
  - 2.10.2 Switch Binding 403
- 2.11 SANtegrity Authentication 404
  - 2.11.1 CHAP 404
  - 2.11.2 RADIUS 404
- 2.12 Reporting 405
- 2.13 Implementation 405
- 2.14 Setup 406
  - 2.14.1 Management network environment 406
  - 2.14.2 EFCM server installation 407
  - 2.14.3 EFCM server initial configuration 417
  - 2.14.4 EFCM remote client installation 421
  - 2.14.5 Starting the remote EFCM client 427
  - 2.14.6 Firewall considerations 429
  - 2.14.7 Defining EFCM user accounts 433
  - 2.14.8 Assigning user rights 438
  - 2.14.9 EFCM event notification 440
  - 2.14.10 Initial switch network configuration 442
  - 2.14.11 Discovering the switch with EFC Manager 452
  - 2.14.12 Feature installation and licensing 458
  - 2.14.13 Obtaining software, firmware, and documentation 472
  - 2.14.14 Firmware installation 478
  - 2.14.15 Initial switch configuration 491
  - 2.14.16 Connecting fiber optics to switch ports 509
  - 2.14.17 SAN140M interactive port card view 521
  - 2.14.18 Arbitrated loop devices 523
  - 2.14.19 Persist fabric 525
- 2.15 Director partitioning 528
- 2.16 Zoning 531
  - 2.16.1 Why we require zoning 531
  - 2.16.2 Zoning implementation 531
  - 2.16.3 Zoning recommendations 532
  - 2.16.4 Zone member definitions 533
  - 2.16.5 Zone management with zone sets 534

2.16.6 Zoning with EFCM. 537
2.16.7 The Zoning Dialog Box 539
2.16.8 Zones, zone sets, and zoning 540
2.17 SANtegrity binding. 555
2.17.1 Fabric Binding 555
2.17.2 Switch Binding. 560
2.17.3 Port Binding. 566
2.18 SANtegrity Authentication 567
2.19 Multiple switch environment 572
2.19.1 Inter-Switch Link 572
2.19.2 Preferred pathing 574
2.19.3 Open Trunking 575
2.19.4 Long distance 578
2.19.5 Merging 579
2.19.6 Routing and iFCP 579
2.20 iSCSI 579
2.21 FICON 579
2.22 Performance monitoring 580
2.22.1 Real-time. 580
2.22.2 Historic 581
2.22.3 Performance graph 584
2.23 Basic troubleshooting 586
2.23.1 Logs 586
2.23.2 Identifying and resolving hardware symptoms 593
2.23.3 Performing data collection. 596
2.23.4 Identifying the principal switch 598
2.23.5 Performing a port wrap test. 598
2.23.6 Performing a cable wrap test 603
2.23.7 Testing a new fiber 603
2.23.8 Unit beaconing 603
2.23.9 Clearing the system error light 604
2.23.10 Port beaconing 605
2.23.11 Detecting light in a fibre. 605
2.23.12 Fibre Channel trace route 605
2.23.13 Switch factory default reset 605
2.24 FICON quickstart configuration 607
2.25 Hardware Configuration Definition 607
2.25.1 McDATA FICON configuration consideration 609
2.26 Setting up the switch identification 610
2.26.1 Setting the FICON view. 611
2.26.2 Naming the ports. 612
2.26.3 Validating features and installing FICON CUP Zoning 614
2.26.4 Configuring switch parameters 616

2.26.5 Setting the switch offline . . . 619
2.26.6 Setting fabric parameters . . . 620
2.26.7 Zoning . . . 623
2.26.8 Activating FICON CUP Zoning . . . 632
2.26.9 Configuring ISL credits and port speed . . . 634
2.26.10 Enabling FICON Management Server (CUP) . . . 636
2.26.11 Setting preferred paths . . . 637
2.26.12 Set Open Trunking . . . 639
2.26.13 Configuring the Allow/Prohibit matrix . . . 641
2.26.14 Enabling binding features . . . 642
2.26.15 Enabling port binding . . . 643
2.26.16 Enabling switch binding . . . 644
2.26.17 Enabling Fabric Binding . . . 645
2.26.18 Clearing link alerts . . . 646
2.26.19 Blocking and unblocking ports . . . 647
2.26.20 Data collection . . . 648
2.26.21 Loading firmware . . . 650
2.26.22 Back up and restore configuration . . . 651

Chapter 3. Implementing a SAN with the q-type family . . . 653
3.1 Introducing the IBM TotalStorage Switch SAN10Q-2 . . . 654
3.2 Installation . . . 655
3.2.1 Documentation . . . 655
3.2.2 Installing SANsurfer Switch Manager . . . 658
3.2.3 Installing the Fibre Channel switch . . . 664
3.2.4 Configuring the Fibre Channel switch . . . 678
3.2.5 Firmware update . . . 686
3.2.6 Zoning . . . 692
3.2.7 Performance Viewer . . . 706
3.2.8 Logs and troubleshooting . . . 713

Chapter 4. Implementing a SAN with the Cisco family . . . 725
4.1 Product introduction . . . 726
4.1.1 MDS 9020 Fabric Switch (non-modular) . . . 726
4.1.2 MDS 9120 Multilayer Fabric Switch (non-modular) . . . 726
4.1.3 MDS 9140 Multilayer Fabric Switch (non-modular) . . . 726
4.1.4 MDS 9216(a/i) Multilayer Fabric Switch . . . 726
4.1.5 MDS 9506 Multilayer Director . . . 727
4.1.6 MDS 9509 Multilayer Director . . . 727
4.1.7 MDS 9513 Multilayer Director . . . 727
4.1.8 Operating system . . . 729
4.1.9 Management tools . . . 730
4.2 Hardware . . . 733

- 4.2.1 Port addressing and port modes 734
4.3 Operating system 736
- 4.3.1 Upgrading the SAN-OS 737
- 4.3.2 Upgrade prerequisites 737
4.4 Management Tools 738
- 4.4.1 Launching the CLI 739
- 4.4.2 System requirements for GUI management tools 740
- 4.4.3 Launching Fabric Manager 741
- 4.4.4 Launching Device Manager 747
- 4.4.5 Launching Performance Manager 751
- 4.4.6 Obtaining the latest source files 754
4.5 Security 755
4.6 Implementation 756
- 4.6.1 Initial setup of the Cisco MDS 9000 family 756
- 4.6.2 Preparing to configure the switch 756
- 4.6.3 Connecting to the switch via the serial port. 756
- 4.6.4 Setting up the initial parameters with the setup program 757
- 4.6.5 Upgrading SAN-OS 760
- 4.6.6 Managing licenses 773
- 4.6.7 Managing users. 780
- 4.6.8 VSAN 786
- 4.6.9 Zoning 797
- 4.6.10 Zoning using the CLI 798
- 4.6.11 Zoning using the GUI 802
- 4.6.12 LUN zoning 821
- 4.6.13 Multiple switch environment 822
- 4.6.14 Inter VSAN Routing (IVR) 829
4.7 IP Services 837
- 4.7.1 FCIP 837
- 4.7.2 Creating an FCIP tunnel using the GUI. 841
- 4.7.3 Creating a PortChannel on FCIP tunnels 845
- 4.7.4 iSCSI 849
4.8 Fabric Manager analysis tools. 854
- 4.8.1 Switch Health Analysis 854
- 4.8.2 Fabric Configuration Analysis 855
- 4.8.3 End to End Connectivity Analysis 860
- 4.8.4 FC Ping 862
- 4.8.5 FC Traceroute 864
- 4.8.6 Show Tech Support. 865
- 4.8.7 Cisco Fabric Analyzer 868
- 4.8.8 Monitoring network traffic using SPAN 870
- 4.8.9 System message logging 877
- 4.8.10 Call Home 878

4.9 FICON quickstart implementation 878
4.10 Hardware Configuration Definition 879
    4.10.1 FICON cascading 880
4.11 FICON port numbering on the MDS switches 881
    4.11.1 FICON port number assignment 882
    4.11.2 FC ID allocation. 884
    4.11.3 Port addresses 884
    4.11.4 Implemented and unimplemented port addresses 885
    4.11.5 Reserved FICON port numbering scheme 885
    4.11.6 Installed and uninstalled ports. 885
    4.11.7 FICON port numbering guidelines. 886
    4.11.8 Assigning FICON port numbers to slots 886
    4.11.9 Port numbers for FCIP and PortChannel interfaces 887
4.12 Cisco MDS 9000 Mainframe Package license 888
4.13 FICON VSAN configuration and requirements 890
    4.13.1 FICON VSAN prerequisites. 891
4.14 FICON load balancing. 901
4.15 Static domain ID configuration 903
4.16 Fabric binding configuration 903
4.17 PortChannel configuration. 908
4.18 Moving ports to the FICON VSAN. 918
    4.18.1 CUP management. 921
4.19 Bringing CHPIDs, devices and CUP online. 925
4.20 FICON configuration files 931
    4.20.1 Using DM to prohibit and block ports 935
    4.20.2 Using DM to swap ports 939

Glossary 945

Related publications 965
Redbooks 965
    Other resources 966
Referenced Web sites 966
How to get Redbooks. 967
Help from IBM 967

Index 969

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

© Copyright IBM Corp. 1999-2007. All rights reserved.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

- AIX®
- Enterprise Storage Server®
- Enterprise Systems Architecture/390®
- ESCON®
- Eserver®
- FICON®
- IBM®
- MVS™
- OS/390®
- OS/400®
- PR/SM™
- pSeries®
- Redbooks®
- Redbooks (logo) ®
- RMF™
- S/360™
- S/370™
- S/390®
- Storage Tank™
- System z9™
- System Storage™
- System/360™
- System/370™
- Tivoli®
- TotalStorage®
- xSeries®
- z/Architecture®
- z/OS®
- z/VM®
- zSeries®
- z9™

The following terms are trademarks of other companies:

Acrobat, and Portable Document Format (PDF) are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Java, JavaScript, JRE, Solaris, Ultra, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Excel, Internet Explorer, Microsoft, Visio, Windows NT, Windows Server, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Pentium, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Preface

“Do everything that is necessary and absolutely nothing that is not.”

In this IBM® Redbooks® publication, which is an update and major revision of the previous version, we have tried to consolidate as much of the critical information as possible while covering procedures and tasks that are likely to be encountered on a daily basis.

Each of the products described has much, much more functionality than we could ever hope to cover in just one book. The IBM SAN portfolio is rich in quality products that bring a vast amount of technicality and vitality to the SAN world. Their inclusion and selection is based on a thorough understanding of the storage networking environment that positions IBM, and therefore its customers and partners, in an ideal position to take advantage by their deployment.

We cover the latest additions to the IBM SAN family, which includes products from companies such as Brocade, Cisco, QLogic, and McDATA. We show how they can be implemented in an open systems environment, and we focus on the Fibre Channel protocol (FCP) environment in particular, and a FICON® quickstart section. We address some of the key concepts that they bring to the market, and in each case, we give an overview of those functions that are essential to building a robust SAN environment.

In other Redbooks, we explore in greater depth the IBM SAN product family, Fibre Channel basics, and SAN design concepts. More information can be found in these Redbooks:

- *Introduction to Storage Area Networks*, SG24-5470
- *IBM TotalStorage: SAN Product, Design, and Optimization Guide*, SG24-6384
- *SAN Multiprotocol Routing: An Introduction and Implementation*, SG24-7321

The team that wrote this book

This book was produced by a team of specialists from around the world working at the International Technical Support Organization, San Jose Center.

© Copyright IBM Corp. 1999-2007. All rights reserved.

Jon Tate is a Project Manager for IBM System Storage™ SAN Solutions at the International Technical Support Organization, San Jose Center. Before joining the ITSO in 1999, he worked in the IBM Technical Support Center, providing Level 2 support for IBM storage products. Jon has 21 years of experience in storage software and management, services, and support, and is both an IBM Certified IT Specialist and an IBM SAN Certified Specialist.

Kerry Edwards is a senior accredited IT Specialist within IBM Global Technology Services in the UK. She has over 12 years of IT delivery experience covering a wide range of SAN and storage environments with specific focus on UNIX® based implementations. Her expertise is derived from a mixture of technical project leadership and solid 24x7 support on large UNIX systems. In her current role she provides direction/resolution to critical situations and drives forward key strategic projects to deliver cost savings and service improvements.

Michael Engelbrecht is a Senior IT specialist in IBM Global Technical Services, ITS. He has worked with IBM for 25 years. For the last 5 years he has provided support for South Africa and Africa for storage products, including all SAN products. Before this, he was a networking specialist with many years of networking experience an a large range of networking equipment, specializing in ATM and Frame relay. His is currently level 1 and 2 support, Product Manager, and Educator for zSeries® tape storage, open system tape storage, as well as all SAN switch products for South Africa and Africa. The products are supported from South Africa.

Simon Richardson is a Senior IT Specialist working as a UK Based TR resource within the Integrated Technology Delivery SSO Organization. Before starting his current role in December 2005 he was the Team Lead for all project based delivery for the UK SSO Wintel Team. He has worked at IBM for 10 years. His areas of expertise include Windows® Server Family and xSeries® hardware. Simon is an MCSE and Novell CNE qualified IT Professional.

Thanks to the following people for their contributions to this project:

Tom Cady
Emma Jacobs
Leslie Parham
Deanna Polm
Sangam Racherla
Sokkieng Wang
Yvonne Lyon
International Technical Support Organization, San Jose Center

Lisa Dorr
IBM Storage Systems Group

Khalid Ansari
George DeBiasi
Brian Cartwright
Sven Eichelbaum
Steve Garraway
Cameron Hildebran
Uwe Hofmann
Thomas Jahn
Andy McManus
Jeannie Ostdiek
Pauli Ramo
Glen Routley
Marcus Thordal
Eric Wong
The previous authors of this book

Sam Mercier
Charles Hubert
IBM Systems & Technology Group

Jim Baldyga
Silviano Gaona
Brian Steffler
Brocade Communications Systems

Hui Chen
Dan Hersey
John McKibben
Darshak Patel
Paul Raytick
Cisco Systems

Brent Anderson (formerly of McDATA)
Jeff Gatz
Prasad Pammidimukkala
McDATA Corporation

Keith Burnett
Nasir Moinuddin
QLogic Corporation

Tom and Jenny Chang
Garden Inn Hotel, Los Gatos, California

Become a published author

Join us for a two- to six-week residency program! Help write one of our Redbooks dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You will have the opportunity to team with IBM technical professionals, Business Partners, and Clients.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you will develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our Redbooks to be as helpful as possible. Send us your comments about this or other Redbooks in one of the following ways:

- Use the online **Contact us** form to review Redbooks, at:

  ibm.com/redbooks

- Send your comments in an e-mail to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Summary of changes

This section describes the technical changes made in this edition of the book and in previous editions. This edition may also include minor corrections and editorial changes that are not identified as created or updated on May 9, 2007.

May 2007, Seventh Edition

This revision reflects the addition, deletion, or modification of new and changed information described below.

New information

- QLogic chapter added

Changed information

- Emulex chapter removed
- Brocade hardware and software information
- McDATA hardware and software information
- Cisco hardware and software information

© Copyright IBM Corp. 1999-2007. All rights reserved.

1

Implementing a SAN with the b-type family

In this chapter we introduce the IBM TotalStorage® SAN b-type family of Fibre Channel switches and directors, which are provided under an OEM agreement with Brocade. We include the full range of products and detail the steps required to install and configure a fabric, and to perform basic management functions, including upgrading firmware, implementing a secure fabric, and monitoring performance within the fabric. We also introduce some basic troubleshooting techniques.

> **Note:** For the various manuals mentioned in this chapter, refer to the version that relates to your version of Fabric Operating System and Fabric Manager.

© Copyright IBM Corp. 1999-2007. All rights reserved.

1.1 Product introduction

In the sections that follow we describe the IBM TotalStorage b-type family of SAN products.

1.1.1 Hardware

The b-type fabric directors and switches provide a flexible, intelligent platform for networking storage. With models ranging from entry-level 8-port fabric switches to 256-port directors, this family addresses the requirements of small departments and global enterprises alike. The 1, 2, and 4 Gbps solutions are available to support high-performance requirements. Express models that are pre-configured with Small Form-factor Pluggable (SFP) optical transceivers are available for several of the switches within the b-type family.

In Table 1-1 we list the b-type family products, along with their equivalent Brocade names.

Table 1-1 IBM TotalStorage SAN b-type product family

IBM name	IBM machine type and model	Brocade name
IBM TotalStorage SAN16B-2	2005-B16	SilkWorm 200E
IBM TotalStorage SAN32B-2	2005-B32	SilkWorm 4100
IBM TotalStorage SAN64B-2	2005-B64	SilkWorm 4900
IBM TotalStorage M14	2109-M14	SilkWorm 24000
IBM TotalStorage SAN256B	2109-M48	SilkWorm 48000

The b-type family also includes the SAN16B-R, SAN18B-R routers as well as the FR4-18i router blade for the SAN256B director. These are discussed in depth in *SAN Multiprotocol Routing: An Introduction and Implementation*, SG24-7321.

Note: We reference the switches via their standard IBM names as well as the IBM type/model throughout this text.

IBM TotalStorage SAN16B-2 fabric switch

Figure 1-1 shows the SAN16B-2 switch.

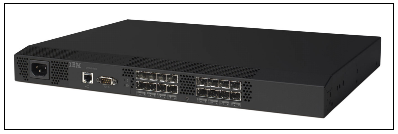


Figure 1-1 SAN16B-2 Fabric switch

The SAN16B-2 is a high performance, scalable, and simple-to-use fabric switch designed to be the foundation for small to medium-size SANs. It provides an 8, 12, or 16 port 4 Gbps fabric for servers running Microsoft® Windows, UNIX, Linux®, NetWare, and OS/400® operating systems, server clustering, infrastructure simplification and business continuity solutions. The SAN16B-2 includes EZSwitchSetup Wizard, an easy-to-use configuration wizard designed to simplify setup and ongoing maintenance for novice users. The base switch offers WebTools and Advanced Zoning with 8 ports activated.

Optional Ports-on-Demand is available in 4 port increments, and full fabric participation with E_Port upgrade is required to connect to other switches. Optional advanced functions are available for intelligent SAN management and monitoring plus full participation in an IBM TotalStorage SAN b-type extended fabric.

IBM TotalStorage SAN32B-2 fabric switch

Figure 1-2 shows the SAN32B-2 fabric switch.

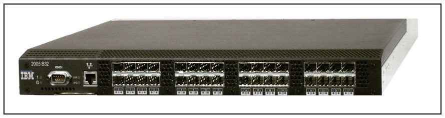


Figure 1-2 SAN32B-2 Fabric switch

A high performance midrange fabric switch which provides 16, 24, and 32-port, 4 Gbps fabrics switching for Windows NT/2000 and UNIX server clustering, infrastructure simplification and business continuity solutions. The base switch offers Advanced Zoning, Full Fabric License, Fabric Watch, WebTools, NPIV software, dual replaceable power supplies and 16-ports activated. The Ports on Demand features support “pay-as-you-grow” scalability in 8 port increments.

IBM TotalStorage SAN64B-2

Figure 1-3 shows the SAN64B-2 fabric switch.

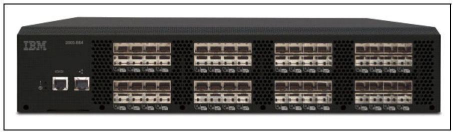


Figure 1-3 SAN 64B-2 Fabric switch

The SAN64B-2 is designed for high performance and also supports high availability. It has redundant, hot-swappable fans, power supplies, and provides the ability to implement non-disruptive software upgrades. The primary advantage of this switch is that it provides a port dense switch to fulfill midrange SAN requirements. The "pay-as-you-grow" Ports on Demand options create a flexible and scalable switch that can meet the requirements of medium sized SANs. The switch comes configured with 32 ports as standard, with optional 16 port extensions providing 48 and 64 port configurations. The ports support 1, 2, and 4 Gbps link speeds and with Inter-Switch Link (ISL) trunking speeds of up to 32 Gbps per data path can be achieved. Advanced Zoning, Full Fabric License, WebTools, Fabric Watch, and NPIV software are provided as standard.

IBM TotalStorage M14 SAN Director

The IBM TotalStorage M14 SAN Director is a high availability enterprise director providing from 32 to 128 ports in a single fabric. This product provides 2 Gbps fabric switching for Windows NT/2000 and UNIX; and FICON switching for mainframe server clustering, infrastructure simplification and business continuity solutions. The base director includes Advanced Zoning, WebTools, Fabric Watch, ISL-Trunking and Performance Monitoring. The Fabric Manager feature can simplify complex fabric management.

IBM TotalStorage SAN256B SAN Director

Figure 1-4 shows the SAN256B SAN Director.

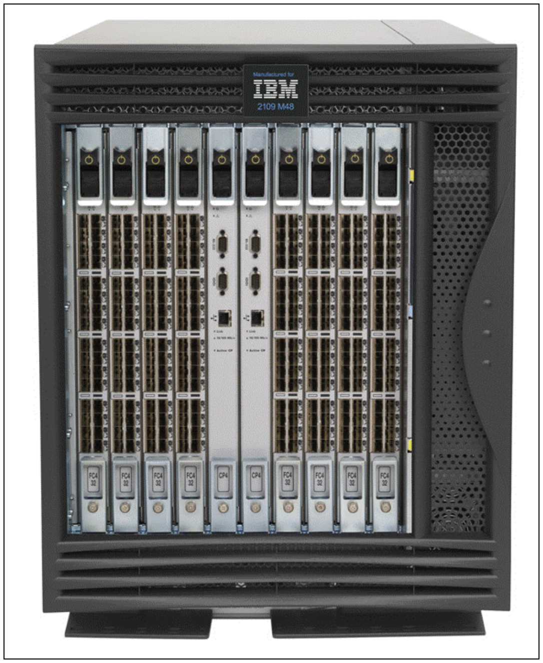


Figure 1-4 256B SAN Director

This next generation of high performance, high density, and high availability SAN directors is designed to be the foundation for large enterprise-class infrastructure simplification and business continuity solutions. The SAN256B director provides from 16 to 256 ports and contains two control processors for high availability and from one to eight blades, each of which contains either 16 or 32 ports.

Each port can support 4, 2 or 1 Gbps link speeds. Standard features include Advanced Inter-Switch Link (ISL) Trunking, WebTools, Advanced Zoning, Fabric Watch, and Performance Monitoring. with optional features including Extended Fabric Activation, Advanced Security Activation and FICON with CUP, these can support a wide range of advanced SAN management, as well as extended fabric and security requirements. The SAN256B can serve as both the core or edge building block in an IBM TotalStorage b-type fabric or as a high-density stand-alone director, providing investment protection and configuration flexibility.

Table 1-2 and Table 1-3 provide an overview of the standard hardware and software available on the b-type switches and also detail some of the options that can be purchased.

Key:

- F - Fixed
- HS - Hot Swappable
- Y - Yes
- O - Optional
- S - Standard

Table 1-2 Hardware features

Features	**SAN16B-2**	**SAN32B-2**	**SAN64B-2**	**SAN256B**
Size	1U	1U	2U	14U
Power Supply	1F	2 HS	2 HS	2-4 HS
Fans	3 F	3 HS	3 HS	3 HS
“Pay as you grow” - Ports on Demand - port activation options	4	8	16	N/A
SWL and LWL SFPs	Y	Y	Y	Y

Table 1-3 Software details

Features	**SAN16B-2**	**SAN32B-2**	**SAN64B-2**	**SAN256B**
EZSwitchSetup Wizard	S	N/A	N/A	N/A
WebTools	S	S	S	S
Advanced Zoning	S	S	S	S
Full Fabric License	O	S	S	S
Brocade Fabric Watch	O	S	S	S
Performance Bundle (ISL Trunking, Advanced Performance Monitoring)	O	O	O	S
Brocade Extended Fabrics	O	O	O	O
Advanced Security - Secure Fabric OS	O	O	O	O
Brocade FICON CUP	N/A	O	O	O

1.1.2 Fabric Operating System

Fabric Operating System (FOS) provides enterprise-class, ultra-high availability, reliability, and security capabilities for a wide range of SAN environments. Fabric OS runs on the b-type SAN family of Fibre Channel directors and switches, providing transparent interoperability between 1, 2, and 4 Gbps devices as well as the reliable, high-performance data transport that is critical for scalable SAN fabrics interconnecting thousands of servers and storage devices. FOS version 5.x is common across all current members of the IBM TotalStorage SAN b-type family and supports up to 2560 ports and 56 domains in single fabric.

1.1.3 Management tools

To ensure open fabric management, Fabric OS provides standard management interfaces, a full range of management tools, and an API that enables the development of third-party SAN management applications. The following tools simplify SAN fabric management by centralizing control and increase efficiencies by enabling automation of repetitive administrative tasks:

- **WebTools:** A built-in Web-based application providing administration and management functions on a per switch basis.
- **Fabric Manager:** A Client/Server-based external application allowing advanced administration of multiple fabrics.
- **Fabric Watch:** A FOS built-in tool that allows the monitoring of key switch elements: power supplies, fans, temperature, error counters and so on.
- **SNMP:** The Simple Network Management Protocol (SNMP) enables storage administrators to manage storage network performance, find and solve storage network problems, and plan for storage network growth.

1.1.4 Licensing

Within the b-type SAN family, licensing is performed at both a hardware and software level. The “pay-as-you-grow” flexibility with Ports On Demand allows scalability from 8 to 12 or 16 or 32 ports in 4-port, 8-port, or 16-port increments on the entry and midrange products. Features such as Trunking or Advanced Performance Monitoring (APM), Extended Fabrics and Secure Fabric OS are software licensed and available across all platforms.

1.1.5 Security

Security within Storage Area Networks comes in many flavors: external security, restricting physical access to directors and switches; software-based, where with the use of zoning we can restrict which hosts and storage can communicate; and hardware-based, where with the use of frame filtering we can monitor each frame and enforce its path through a SAN fabric. Additionally, Secure Fabric OS (SFOS) is an optionally licensed product that provides customizable security restrictions through local and remote management channels on a b-type fabric.

SFOS provides the ability to create policies to customize fabric management access, specify which switches and devices can join the fabric, view statistics related to attempted policy violations, manage the fabric-wide SFOS parameters through a single switch, create temporary passwords specific to a login account and switch, and enable and disable SFOS as desired.

SFOS uses digital certificates-based on PKI or Diffie-Hellman with Challenge-Handshake Authentication Protocol (DH-CHAP) shared secrets to provide switch-to-switch authentication. There is also support for the Secure Socket Layer (SSL) protocol and Secure HTTP (HTTPS).

1.1.6 Support

The Brocade Assist Web site provides support for IBM users, this can be accessed at:

`http://ibm.brocadeassist.com`

1.2 The hardware

The IBM TotalStorage SAN Switch b-type family of products provide a range of entry and midrange switches and enterprise class directors. The entry level, midrange, and director models provide 1, 2 and 4 Gbps port-to-port non-blocking throughput with auto-sensing capability for connecting to older 1 Gbps host servers, storage, and switches. Unlike hub-based Fibre Channel Arbitrated Loop (FC-AL) solutions, which reduce performance as devices are added by sharing the bandwidth, an IBM TotalStorage SAN Switch Fabric throughput continues to increase as additional ports are interconnected.

All of these models are fully interoperable with the previous IBM TotalStorage SAN Switches, and can be added to existing fabrics, enabling transition from existing Fibre Channel storage networks to the faster technology.

In Table 1-4, we list the current and historic switch/director model types with speed and port capabilities, the current supported version of FOS, and the type of Application Specific Integrated Circuit (ASIC).

Table 1-4 Director/Switch models

Switch type	# Ports	Port speed	FOS version	ASIC type
2005-B16	8, 12, or 16	1, 2 and 4Gb/s	5.1.x	Goldeneye
2005-B32	16, 24 or 32	1, 2 and 4Gb/s	5.1.x	Condor
2005-B64	32, 48 or 64	1, 2 and 4Gb/s	5.1.x	Condor
2109-M48	16 to 256	1, 2 and 4Gb/s	5.1.x	Condor
2109-M14	32 to 128	1 and 2Gb/s	5.1.x	Bloom II
2109-M12	16 to 64	1 and 2Gb/s	5.0.x	Bloom
2005-H16	16	1 and 2Gb/s	5.1.x	Bloom II
2005-H08	8	1 and 2Gb/s	5.1.x	Bloom II
2109-F32	32	1 and 2Gb/s	5.1.x	Bloom
2109-F16	16	1 and 2Gb/s	3.2.x	Bloom
3534-F08	8	1 and 2Gb/s	3.2.x	Bloom
2109-S16	16	1Gb/s	2.6.x	Loom
2109-S08	8	1Gb/s	2.6.x	Loom
3534-1RU	8	1Gb/s	2.6.x	Loom

1.2.1 Generic features

In the following paragraphs, we describe some of the standard features available on all of the b-type family.

Auto-sensing speed negotiation

The IBM TotalStorage SAN Switch uses internal Application Specific Integrated Circuits (ASICs) supporting link operation at either 4 Gbps or 2 Gbps or 1 Gbps. As a device is connected to a port, the link speed is negotiated to the highest speed that is supported by the device. This speed selection is auto-negotiated by the ASIC driver on a per-port basis. If multiple devices are connected to a port (for example, on an FL_Port), the driver auto-negotiates for the highest common speed and sets the transmitter and receiver accordingly. This auto-sensing negotiation allows easy configuration.

Frame filtering

Zoning is a fabric management service that can be used to create logical subsets of devices within a SAN and enable partitioning of resources for management and access control purposes. Frame filtering enables the switch to provide zoning functions with finer granularity. Frame filtering can be used to set up port level zoning, world wide name zoning, device level zoning, protocol level zoning, and LUN level zoning. After the filter is set up, the complicated function of zoning and filtering can be achieved at wire speed. Frame filtering is also used with performance monitoring, allowing you to monitor either "End to End" traffic flow or device-based I/O requirements.

Routing

The switch or director's control processor maintains two routing tables, one for unicast and one for multicast. The unicast routing tables are constructed during fabric initialization. The multicast tables are initially empty, except for broadcast addresses. When the tables have been constructed, they are loaded into each ASIC.

The unicast tables change if ports or links come online or go offline, or if some other topology changes occur. These updates are triggered by a Resource State Change Notification (RSCN). When new paths become available, the control processor can change the routing tables in order to share the traffic load.

The multicast tables change as ports register with the alias server to create, join, or leave a multicast group. Each time a table changes, it must be reloaded into the ASICs.

Service functions

The ASIC interrupts the embedded processor when a frame arrives that has an error (for example, incorrect source ID), when a frame times-out, or when a frame arrives for a destination that is not in its routing tables. In the latter case, the frame might be addressed to an illegal destination ID, or it might be addressed to one of the service functions that are provided by the embedded processor such as SNMP, name server, or alias server.

ISL Trunking

The current IBM TotalStorage b-type switches have an optional feature called ISL Trunking. ISL Trunking is ideal for optimizing performance and simplifying the management of a multi-switch SAN fabric.

When two to four or eight adjacent ISLs in the same trunking group, depending on switch models, are used to connect two switches, the switches automatically group the ISLs into a single logical ISL, or *trunk*. The throughput of the resulting trunk is the sum of the throughputs of the participating links.

ISL trunking is designed to significantly reduce traffic congestion. As shown in Figure 1-5, four 4 Gbps ISLs are combined into a single logical ISL with a total bandwidth of 32 Gbps. The trunk can support any number of connections, although we only show five connections in our example. Be aware that prior to implementing the trunking, the four parallel ISLs result in a throughput of 10 Gb due to the fact that two of the connections are sharing the same ISL. Following the implementation of trunking, this throughput increases to 14 Gb, that is, full throughput.

To balance the load across all of the ISLs in the trunk, each incoming frame is sent across the first available physical ISL in the trunk. As a result, transient workload peaks for one system or application are much less likely to impact the performance of other devices of the SAN fabric.

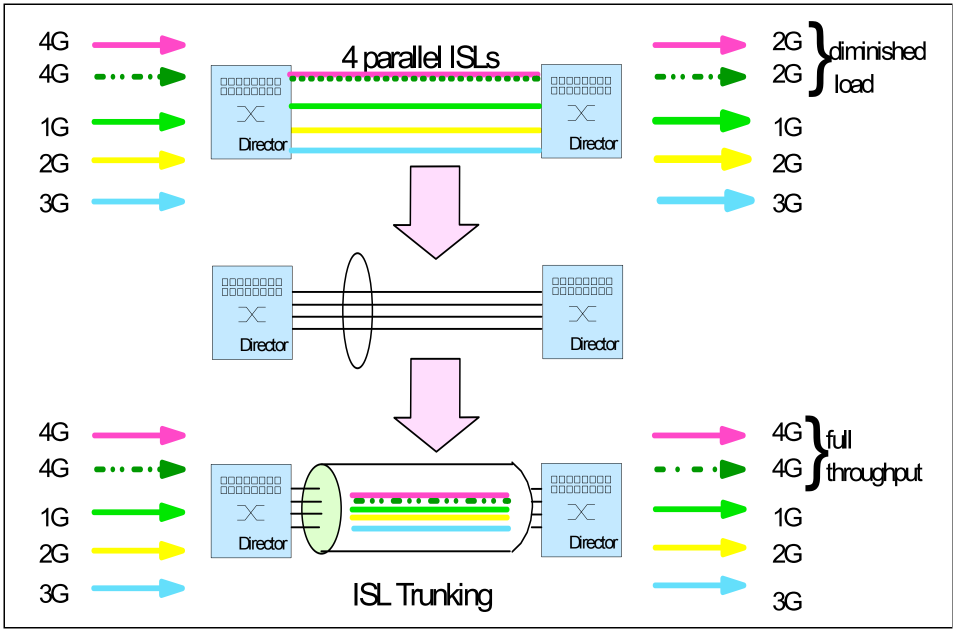

4G
4G
1G
2G
3G
4 parallel ISLs
Director
Director
2G
2G
diminished load
1G
2G
3G
Director
Director
4G
4G
1G
2G
3G
Director
Director
ISL Trunking
4G
4G
full throughput
1G
2G
3G

Figure 1-5 SAN b-type ISL trunking

Because the full bandwidth of each physical link is available with ISL trunking, no bandwidth is wasted by inefficient load sharing. As a result, the entire fabric is used more efficiently. Fabric OS and management software, such as Fabric Watch, also view the group of physical ISLs as a single logical ISL. A failure of a single ISL in a trunk causes only a reduction of the available bandwidth and not a failure of the complete route. Therefore, no re-calculation of the routes at that time is required. Bandwidth is automatically restored when the ISL is repaired.

Note: If an older 2 Gbps switch is involved in either end of a trunk, one of the links forming the trunk is chosen as the trunk master. If that trunk master link fails, the trunk must select a new master, causing a slight disruption to traffic. Trunks between the new 4 Gbps switches do not have this restriction.

ISL trunking helps to simplify fabric design, lower provisioning time, enhance switch-to-switch performance, simplify management, and improve the reliability of the SAN fabrics. In-order delivery is still guaranteed by the switch ASICs.

The maximum number of ISLs supported in a single trunk, as well as the maximum trunk speed for different IBM TotalStorage b-type switch models, is detailed in Table 1-5. If you have to form an ISL trunk between two different switch models, the lower of the maximum values for both number of ports supported and port speed apply.

Table 1-5 Maximum trunk capacity

Device type	Ports/trunk	Port speed	Trunk speed
SAN16B-2	4	4 Gbps	16 Gbps
SAN32B-2	8	4 Gbps	32 Gbps
SAN64B-2	8	4 Gbps	32 Gbps
M14	4	2 Gbps	8 Gbps
SAN256B	8	4 Gbps	32 Gbps

Diagnostics

The switch supports a set of power-on self tests (POSTs), as well as tests that can be invoked using a command line interface. These diagnostics are used during the manufacturing process as well as for fault isolation of the product in customer installations. The POST and diagnostic commands concentrate on the Fibre Channel ports and verify the functionality of the switch. Post diagnostics are written to run in the FOS environment. However, as the FOS does not run without a working SDRAM, a SDRAM/boot EEPROM test is run as part of the pre-FOS startup code to verify that the basic processor connected memories are functioning properly.

Loop-back paths for frame traffic are provided in the hardware for diagnostic purposes. A loop-back path within the ASIC, at the final stages of the Fibre Channel interface, can be used to verify that the internal Fibre Channel port logic is functioning properly, as well as paths between the interface and the central memory.

Additionally, the Serial Link macro within the ASIC includes a serial data loop-back function that can be enabled through a register in the corresponding ASIC.

Diagnostics are provided to allow traffic to be circulated between two switch ports that are connected with an external cable. This allows the diagnostics to verify the integrity of the final stage of the SERDES interface, as well as the SFP module.

1.2.2 New features

With the introduction of both the Condor and GoldenEye ASICs, we now have support for 4 Gbps port throughput capability throughout the current product range from the 8-port B16 switch to the 256 port M48 director. Additional functionality of these ASICs provides larger trunking capabilities, integrated SERDES, and exchange-based path selection. The support for these new features is discussed in the following sections.

2005-B16

The 2005-B16 (also known as the SAN16B-2) switch is a single replacement for the 2005-H08 and 2008-H16 model switches. By default, this machine ships with an 8-port license which can be increased in 4-port increments up to 16 ports, using the Pay on Demand (POD) service. All ports can auto negotiate between 1, 2, and 4 Gbps with use of the new tri-rate SFP optics. This box does not ship with a full fabric license and therefore does not support the E_Port functionality, however, once a full fabric license has been purchased, the B16 can be added to an existing fabric.

With the new GoldenEye ASIC, and with support from FOS 5.x, this machine can take advantage of the enhanced trunking functionality to support up to 16 Gbps on an ISL Trunk (with the ISL Trunking license). Other software features (as standard) include WebTools for simple remote administration, Advanced Zoning, and a new EZ switch setup Wizard CD, which greatly simplifies the initial setup of this B16 switch. The EZ switch setup wizard is discussed further in 1.7.4, “SAN16B Quick Setup with EZSwitchSetup v2.1.0” on page 61.

The optional features available for the SAN16B-2 include a Performance Bundle, containing both ISL Trunking and Advanced Performance Monitoring support; Full Fabric, which includes E_Port support, Fabric Watch, and Secure Fabric OS. This product now includes Long Distance Extended Fabric support. Finally, Ports on Demand (POD) support is optional, allowing access to all 16 ports on this machine. Many of these new features are discussed and implemented later within this chapter.

SAN256B

The IBM TotalStorage SAN256B (2109-M48) director is a single domain 256 port machine capable of running its ports at 1, 2, or 4 Gbps. The M48 includes support for FICON, FICON/Fibre Channel intermixing, FICON CUP, and FICON cascading, enabling it to address the demands for integrated zSeries and open system server enterprise SANs. The chassis includes two control processor blades and with improved port density enables up to 256 ports in 14U space. Other standard software features include WebTools, Zoning, Fabric Watch, Trunking and Advanced Performance Monitoring. Optional software products include Extended Fabric Activation, FICON with CUP Activation, and Advanced Security Activation.

Hardware options include 16-port blades that support 1, 2, or 4 Gbps on a port by port basis, or a 32-port blade with the same port-speed options. Although this SAN256B machine supports up to four Power Supply Units (PSUs), only two are required to function in redundant power mode. The chassis also ships with a new cable management tray allowing for more efficient cable routing.

The control processor (CP4) cards are new by design, including faster processor units and make use of two 32-port Condor ASICs as the switching core.

The 16 and 32-port cards make use of cut-through routing ensuring that frames destined for ports on the same card never leave the ASIC. This integrated feature called local switching provides significant performance benefits.

SAN256B numbering scheme

The SAN256B (2109-M48) uses a numbering scheme that progresses from left to right and bottom to top in numerical order. The reference location is from the cable side to chassis:

- Blade assemblies are numbered from 1-10, from left to right.
- Power supplies are numbered from 1-4, from bottom to top.
- Fans are numbered from 1-3, from left to right.
- The physical ports of the 16-port card are numbered 0-15, from bottom to top.
- The physical ports of the 32-port card are numbered 0-15 on the left column and 16-31 on the right column, from bottom to top.

The logical decimal port numbering for the SAN256B with 32-port cards is shown in Figure 1-6.

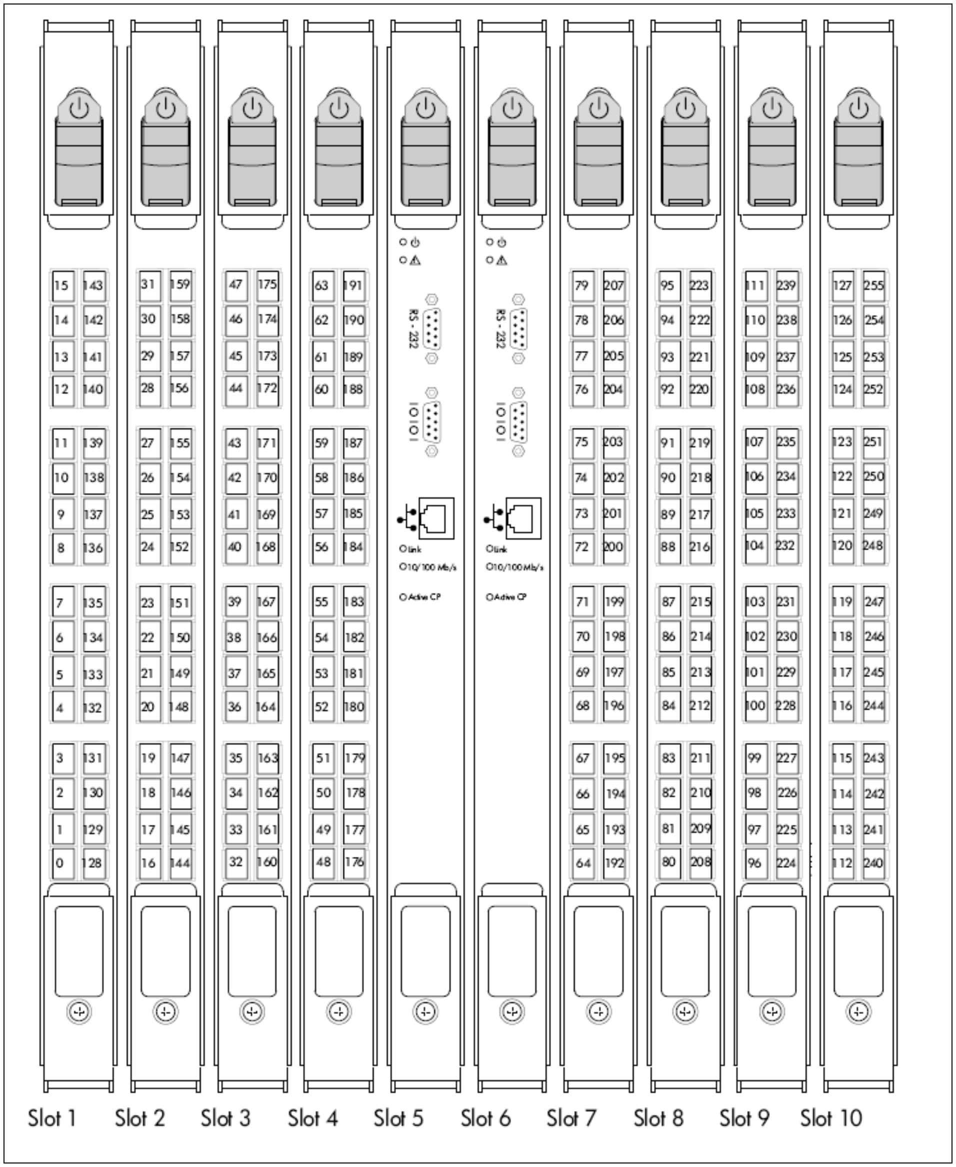

15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
143 142 141 140 139 138 137 136 135 134 133 132 131 130 129 128
31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16
159 158 157 156 155 154 153 152 151 150 149 148 147 146 145 144
47 46 45 44 43 42 41 40 39 38 37 36 35 34 33 32
175 174 173 172 171 170 169 168 167 166 165 164 163 162 161 160
63 62 61 60 59 58 57 56 55 54 53 52 51 50 49 48
191 190 189 188 187 186 185 184 183 182 181 180 179 178 177 176
RS - 232
IOIOI
link
10/100 Mb/s
Active CP
RS - 232
IOIOI
link
10/100 Mb/s
Active CP
79 78 77 76 75 74 73 72 71 70 69 68 67 66 65 64
207 206 205 204 203 202 201 200 199 198 197 196 195 194 193 192
95 94 93 92 91 90 89 88 87 86 85 84 83 82 81 80
223 222 221 220 219 218 217 216 215 214 213 212 211 210 209 208
111 110 109 108 107 106 105 104 103 102 101 100 99 98 97 96
239 238 237 236 235 234 233 232 231 230 229 228 227 226 225 224
127 126 125 124 123 122 121 120 119 118 117 116 115 114 113 112
255 254 253 252 251 250 249 248 247 246 245 244 243 242 241 240
Slot 1
Slot 2
Slot 3
Slot 4
Slot 5
Slot 6
Slot 7
Slot 8
Slot 9
Slot 10

Figure 1-6 IBM TotalStorage SAN256B director 256-port numbering scheme

1.3 Operating system

In this section we describe the software for the IBM TotalStorage SAN Switches.

1.3.1 Fabric Operating System

The Fabric Operating System (FOS) manages the operation of the switch and delivers the same, and compatible, functionality to all the different models of switches and directors. The switch firmware is designed to make the switches easy to install and use while retaining the flexibility required to accommodate user requirements.

The FOS includes all the basic switch and fabric support software as well as optionally licensed software that is enabled using license keys. It is composed of two major software components: firmware that initializes and manages the switch hardware, and diagnostics.

Fabric OS (FOS) Version 5.x and 4.x are Linux-based operating systems, while the FOS Version 3.x and prior were based on the VxWorks operating system. We show the models and required Firmware versions in Table 1-4 on page 9.

New to FOS 5.x

We discuss the new features of FOS 5.x in the following topics.

Staged Port Bring Up

Simply stated, Staged Port Bring Up reduces the number of ports per switch/director type which come online at the same time after a reboot or power on. This new functionality helps to improve the stability of your fabric. If a 256-port fully populated director had all 256 ports enabled at the same time into an existing multi switch fabric, the number of FLOGI requests, SCR requests, and RCSN traffic could be such that it might effectively slow down existing administrative tasks on that SAN network. However, with the introduction of Staged Port Bring Up, in our 256-port director example, we enable 64-port blocks with a staging interval of 500 milliseconds and therefore help reduce the chance of traffic congestion.

The SAN256B (2109-M48) brings up 64 ports per stage, the 2109-M14 enables 32-ports per stage, and the 2109-M12 activates 16-ports per stage. All other switches running FOS 5.x enable 16-ports per stage.

Masterless Trunking

Within the previous generation of b-type products: 2109-F08, 2109-F16, 2109-F32, 2005-H08, 2005-H16, 2109-M12, and 2109-M14 we saw trunking implemented using a Master and Slave type architecture. In the scenario of a slave link failing, no disruption was seen. However, if a Master link were to fail, then a new Master had to be selected, and during this process a minor fabric disruption occurred.

On the current 4 Gbps product set, we see the implementation of a “masterless” trunk. Here, a master is still selected, which is usually the first link up, and is used in the routing tables. However, if this master fails or goes offline, then a slave link immediately becomes the master. Actually, the slave link with the lowest back-port World Wide Name (WWN) is chosen. Therefore, when a master fails, a trunk does not have to be rebuilt, and therefore there is no disruption to traffic, and no disruption to the fabric.

Frame Distribution

With the 2 Gbps b-type product range (F08/F16, H08/H16, M12/M14), I/O traffic was spread across all trunk links regardless of the total load. For example, if we take a 4-member trunk with an 80 MBps traffic load, we might see the traffic distributed as follows: 24 MBps, 16 MBps, 10 MBps and 30 MBps.

However, a single member of this trunk group could have easily handled the total traffic throughput of 80 MBps. Distributing traffic across multiple links is nice for customer demonstrations; however, it is not necessary in a production environment unless one of these single members of the trunk group is nearing its maximum bandwidth.

So, with the Frame Distribution functionality, we see in the 4 Gbps products (FC4 Cards from the M48, the B64, B32, and B16) the individual links within a trunk “fill up” before further traffic is distributed across the remaining links within that trunk. The individual link threshold is set to around 90% utilization before traffic “spills over” to the next link in the trunk.

There are no adverse performance or management effects with this new functionality; no “hot spots” are seen across links, and multi-link trunks are managed as a single link.

Extended ISL Trunking

A limitation of the previous trunking architecture was the maximum distance a trunk could extend, that of only 5 km at 2 Gbps. With Extended ISL trunking, we can now extend our trunks to distances up to 250 km, and at 1 Gbps we can have a full performance, long distance ISL of 500 km. There are some guidelines as to how these extended distances are implemented. All ports in the same trunk group must have similar cable lengths and have the same distance setting (LD, L1, and so on). IBM recommends a difference of 30 meters or less as the total difference in cable lengths, however there is a maximum total cable length difference, and this is a hard stop, of 400 meters. The current set of trunk-based CLI commands remains the same: **`trunkShow`**; **`trunkDebug`**; **`switchshow`**; **`portCfgtrunkport`**; **`portCfgshow`**. Table 1-6 shows some of these capabilities.

Table 1-6 Current capabilities of trunks

Mode	Distance	4G ports, or trunks	2G ports, or trunks	1G ports
LE	10 km	32 ports, or Four 8-port	32 ports, or Four 8-port trunks	32 ports
L0.5	25 km	15 ports, or One 8-port	32 ports, or Four 8-port trunks	32 ports
L1	50 km	7 ports, or One 7-port trunk	15 ports, or One 8-port trunk	32 ports
L2	100 km	3 ports, or One 3-port trunk	7 ports, or One 7 port trunk	15 ports
LD	200 km	0	3 ports, or One 3-port trunk	7 ports
LD	250 km	0	3 ports, or One 3-port trunk	6 ports
LD	500 km	0	0	3 ports

Dynamic Path Selection

In addition to ISL Trunking, most members of the IBM TotalStorage b-type family implement an additional load-balancing scheme, called Dynamic Path Selection (DPS). DPS can balance traffic over up to eight equal-cost paths. The paths can each be either ISLs or trunk groups.

Every Fibre Channel frame contains three data fields relevant to routing:

- Source PID (SID)
- Destination PID (DID)
- Exchange ID (OXID)

In normal operation, any frames relating to the same SCSI operation have the same exchange ID.

If DPS is not used, all traffic between any single SID and DID pair is always routed via the same path. This static relation can cause the division of traffic between ISLs or trunk groups to be less than optimal. However, this functionality also guarantees in-order delivery of any FC frames between the SID and DID pair.

If DPS is used, one path from the set of equal-cost paths is chosen for every exchange, based on formula using SID, DID, and OXID. All frames of the same exchange use the same path. The different exchanges between the same SID and DID are striped across all available paths, effectively balancing the load across them. This functionality still guarantees in-order delivery of any FC frames within any given exchange. Frames belonging to different exchanges can potentially arrive out-of-order.

DPS supports operation on any ISL or trunk group, independent on ASIC, port group, or port card boundaries. It can be even used at edge switches for load-balancing between different core switches or directors in a core-to-edge fabric, as shown in Figure 1-7.

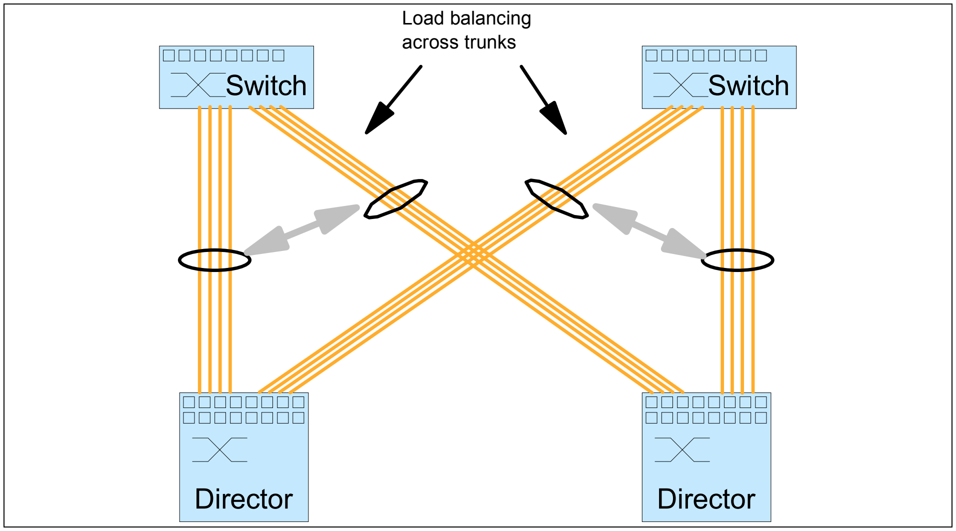


Figure 1-7 Dynamic Path Selection in core-to-edge fabrics

DPS can support distances that are too long for ISL Trunking, as well as paths with different latency, such as cables with different routes.

Note: The exchange-based routing policy is the default policy for any switches that support DPS. For FICON environments, you have to change these switches to use the device-based routing policy, where the routes are chosen by only SID and DID.

The current models supporting DPS include SAN-16B, SAN-32B, SAN-64B, and SAN256B. Figure 1-8 shows another example of DPS.

Load sharing and load balancing: Non-trunked, parallel ISLs always share load, or traffic, in a rough, server-oriented way. The next server gets the next available ISL, regardless of the amount of traffic each server is generating. Load balancing, however, is the means to find an effective way to use all of the cumulative bandwidth of the parallel ISLs.

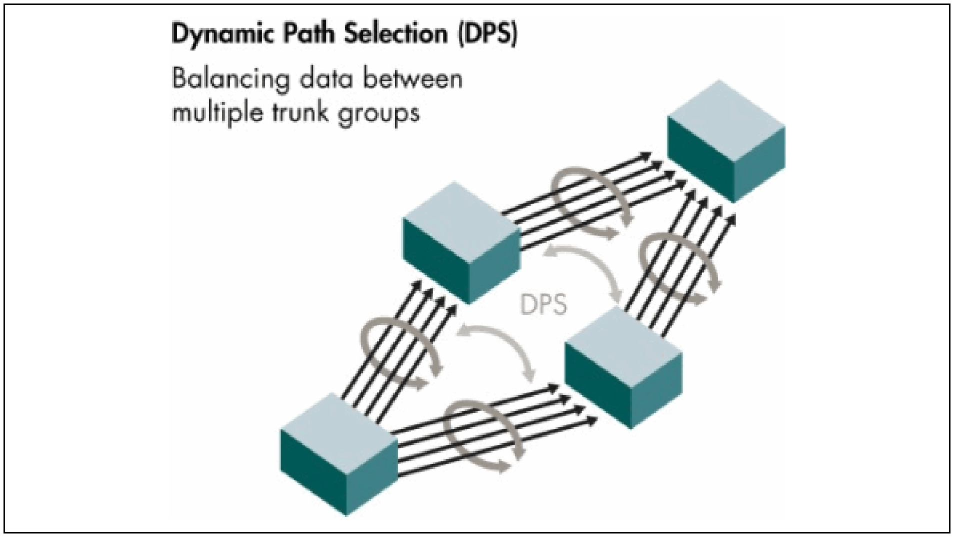

Dynamic Path Selection (DPS)
Balancing data between multiple trunk groups
DPS

Figure 1-8 Dynamic Path Selection example

Routing policies

In the previous generations of b-type switches, we used port-based routing. Today, with FOS 5.x and 4 Gbps hardware, we are able to optimize our routing policies by using either device-based routing or exchange-based routing. In fact, exchange-based routing is now the default with 4 Gbps hardware. It can be changed where necessary using the **`aptpolicy`** command, but the switch must be disabled before changing the policy.

In Example 1-1 we change the routing policy to Exchange-Based Routing Policy:

Example 1-1 Changing the routing policy using aptpolicy

```
IBM_2005_B32:admin> switchdisable
IBM_2005_B32:admin> aptpolicy 3
Policy updated successfully.
IBM_2005_B32:admin> switchenable
IBM_2005_B32:admin> aptpolicy
 Current Policy: 3

 3: Default Policy
 1: Port-Based Routing Policy
 2: Device-Based Routing Policy
 3: Exchange-Based Routing Policy
```

Port-based routing, or flow, uses both the source ID (SID) and destination ID (DID) as routing information, and paths remain the same for all exchanges. This type of routing is devised for FICON environments.

Exchange-based routing, or flow, also uses SID and DID but includes the exchange ID (OXID) in its routing. Exchanges are equivalent to a SCSI IO (SCSI Read or Write). Here the path might change with every SCSI command.

In both routing policies, in-order delivery is guaranteed for frames within a flow, for example: CCW FICON, SCSI commands, or management commands. Both policies ensure that all paths are used optimally.

Extended Distance Support

With the introduction of FOS 5.1.0, extended fabric support is now also an option on the SAN-16B switch. It is important to observe that Extended Fabric does not work if the long distance ISL is installed between non-matching edge port switches. This only becomes an issue if we are implementing ISLs across the older 1 Gbps switches, specifically the Extended ISL support for the IBM 3534-1RU, 2109-S08 and 2109-S16 series switches is limited as follows: Extended ISLs are not supported between IBM 3534-1RU, 2109-S08 and 2109-S16 switches and other 2109 and 2005 models.

When mixing switch types in an extended distance environment, the supported distance is the lowest common denominator; for example, a SAN32B to an M14 is limited to 100 km at 2 Gbps as this is the maximum distance of the M14, in this case the lowest common denominator.

When initiating long distance links, we use the **`portcfglongdistance`** command to set up the ports at each end of the link. In FOS 5.x we see an additional operand added to this command:

```
portcfglongdistance <portnumber>, “distance level”, [vc_translative_init],
<max_distance>
```

A new, mandatory operand, **`max_distance`**, is used when setting links distance level to LD. The **`max_distance`** operand represents the maximum distance in kilometers of the extended link. This new functionality helps the switch or director to determine the proper amount of buffer allocation, and therefore ensuring the LD port from being short of buffers.

Notice that the LD mode does determine the exact number of buffer credits at the time of initialization, but if the other ports use up all the buffer credits before the extended LD port initializes, we could have an unstable connection. For example, if 10 ports are configured to use LD mode, and the first 8 ports have used up all the buffer credits, then the remaining 2 LD ports are set into buffer limited mode. Using the **`max_distance`** operand helps to avoid this situation.

If we find ourselves in a situation where the “actual” distance of a link is different from the **max_distance**, then the buffers are allocated to the minimum value of these two settings. For example, if a maximum distance of 30 km is defined and the actual distance is 28 km, the switch uses the actual value (28 km). Both WebTools and the CLI (**portshow**) can be used to view the actual and maximum distance settings.

Be aware that the **portcfglongdistance** command fails if there are not enough buffers available at the time of the setting.

The **portbuffershow** command is new to FOS and shows you on a port by port basis the number of reserved buffers per port, based on the **max_distance** setting, the actual buffer usage, how many buffers are required based on the actual distance, and the remaining buffers for the entire port group.

In Example 1-2 we show the output from the **portbuffershow** command run on a SAN-32B switch:

Example 1-2 Output from the portbuffershow command

```
ITSO_2005_B32:admin> portbuffershow 17
User  Port   Lx   Max/Resv Buffer Needed     Link   Remaining
Port  Type  Mode  Buffers  Usage  Buffers  Distance  Buffers
----  ----  ----  -------  ------ ------- --------- ----------
  0           -       8       0       -        -
  1           -       8       0       -        -
  2    E      -       8      26      26       5km
  3           -       8       0       -        -
  4           -       8       0       -        -
  5           -       8       0       -        -
  6           -       8       0       -        -
  7    F      -       8       8       -        -
  8    E      -       8      26      26       5km
  9           -       8       0       -        -
 10           -       8       0       -        -
 11           -       8       0       -        -
 12           -       8       0       -        -
 13           -       8       0       -        -
 14           -       8       0       -        -
 15           -       8       0       -        -
 16           -       8       0       -        -
 17           -       8       0       -        -
 18           -       8       0       -        -
 19           -       8       0       -        -
 20           -       8       0       -        -
 21           -       8       0       -        -
 22           -       8       0       -        -
 23           -       8       0       -        -
 24    E       -       8      26      26        2km
 25    E       -       8      26      26        2km
 26    E       -       8      26      26        2km
 27    E       -       8      26      26        2km
 28            -       8       0       -        -
 29            -       8       0       -        -
 30            -       8       0       -        -
 31            -       8       0       -        -         636
```

Notice that the **portbuffershow** command, when used with a specific port number, shows the full port listing for the whole of the port group to which that port belongs. In our example this results in all of the switch ports being presented, because we have only one port group which encompasses them all.

Buffer management

In the SAN32B, SAN64B, and FC4 cards within an M48, we use the Condor ASIC. This ASIC has a total of 1024 buffers. These are shared among the 32 ports and the embedded port. Actually, the embedded port takes 24 buffers for management traffic usage. The system automatically allocates these buffers based upon the port topology (E_Port/F_Port/FL_Port).

All ports get a minimum of 8 buffer credits, including the unlicensed ports. A standard E_Port gets 26 buffers, and a maximum of 255 credits with a long distance setting. The Condor ASIC makes use of all 6 long distance settings (L0, LE, L0.5, L1, L2, LD). L0 and LE modes do not require Extended Fabric licenses. For 4 Gbps links between 2.5 km and 10 km, we recommend LE mode for 2 Gbps links between 5 and 10 km we also recommend LE mode.

The GoldenEye ASIC, found in the SAN16B switch, has a total of 288 buffers. These are shared among the 16 ports and the embedded port. LE mode should be used on an E_Port when the link is 4 Gbps and between 1.5 km and 10 km, or on a 2 Gbps link where the distance is between 3 km and 10 km, or on a 1 Gbps link with a distance of 6 km to 10 km.

Buffer limited ports

Buffer limited ports occur when an E_Port or a port in LD mode do not have the optimum number of buffer credits, for example, when an E_Port has less than 26 buffer credits. This situation arises when credits are over-assigned, either due to multiple long-distance settings or not enough credits to match all port long distance configurations. A buffer limited port is assigned 8 credits, and remains limited until there are long distance configuration changes or port speed changes. Buffer limited ports can be found via the CLI using either **switchshow**, **errorshow** , **portshow**, or **portbuffershow** . WebTools shows buffer limited ports in a blue color.

The fcping command

With FOS 5.0.1 we see the introduction of a troubleshooting command that helps diagnose any FC connectivity issues. The command is called **`fcping`**. Its origins stem from the UNIX **`ping`** command.

When we initiate an **`fcping`** command, providing both a source and destination WorldWide Name (WWN), it initially performs a zoning check; then we see an Extended Link Service (ELS) ECHO request sent to both the source and destination devices. These ELS requests are initiated from the b-type embedded port. An **`fcping`** must be initiated from a switch running FOS 5.0.x or above, however the source and destination ports can reside on switches with older versions of FOS.

Best practices dictate that the **`fcping`** should be initiated from a switch that contains either the source or destination device. This way, the ELS ECHO request is most likely to follow the true data frame path. If the **`fcping`** is initiated from a third switch, then the actual path of the ping frame might be different than that of the source/destination path, and therefore the resulting round-trip time might be unexpected.

Example 1-3 details the **`fcping`** command in use.

Example 1-3 The fcping command in use

```
IBM_2005_B32:admin> fcping 10:00:00:00:c9:32:a9:1d 21:00:00:e0:8b:18:55:8e
Source:         10:00:00:00:c9:32:a9:1d
Destination:    21:00:00:e0:8b:18:55:8e
Zone Check:     Not Zoned

Pinging 10:00:00:00:c9:32:a9:1d [0x11000] with 12 bytes of data:
received reply from 10:00:00:00:c9:32:a9:1d: 12 bytes time:594 usec
received reply from 10:00:00:00:c9:32:a9:1d: 12 bytes time:519 usec
received reply from 10:00:00:00:c9:32:a9:1d: 12 bytes time:515 usec
received reply from 10:00:00:00:c9:32:a9:1d: 12 bytes time:779 usec
received reply from 10:00:00:00:c9:32:a9:1d: 12 bytes time:649 usec
5 frames sent, 5 frames received, 0 frames rejected, 0 frames timeout
Round-trip min/avg/max = 515/611/779 usec

Pinging 21:00:00:e0:8b:18:55:8e [0x11200] with 12 bytes of data:
received reply from 21:00:00:e0:8b:18:55:8e: 12 bytes time:519 usec
received reply from 21:00:00:e0:8b:18:55:8e: 12 bytes time:517 usec
received reply from 21:00:00:e0:8b:18:55:8e: 12 bytes time:514 usec
received reply from 21:00:00:e0:8b:18:55:8e: 12 bytes time:516 usec
received reply from 21:00:00:e0:8b:18:55:8e: 12 bytes time:546 usec
5 frames sent, 5 frames received, 0 frames rejected, 0 frames timeout
Round-trip min/avg/max = 514/522/546 usec
```

Port RSCN suppression

The purpose of this functionality is to eliminate unwanted RSCNs directed towards hosts. This ultimately reduces unnecessary and unintentional interruptions of I/O activity. When activating RSCN suppression on a port, any further changes on that port do not generate RCSN traffic to any other devices.

For example, a zone containing multiple hosts that do not communicate with each other inband, you would enable RSCN suppression on all these connected hosts, then reboot one host. No RSCN information is transmitted to any of the remaining hosts in this zone. Of course, implementing a fine granularity of zoning, a single HBA to a single storage device achieves the same effect but entails increased administration time, zone complexity, and increases the zoning configuration size.

RSCN suppression can be configured live and on any port on a b-type switch or director and this configuration is persistent across reboots. However, RSCN suppression is locked to a port, therefore if a device is moved, the new port must be configured and the original port unconfigured.

Port suppression can be displayed from the CLI using the **`portcfgshow`** command, and configured using the **`portcfg`** command. See Example 1-4.

Example 1-4 The portcfgshow command

```
ITSO_2005_B32:admin> portcfgshow
Ports of Slot 0    0  1  2  3    4  5  6  7    8  9 10 11   12 13 14 15
-----------------+--+--+--+--+----+--+--+--+----+--+--+--+----+--+--+--
Speed             AN AN AN AN   AN AN AN AN   AN AN AN AN   AN AN AN AN
Trunk Port        ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
Long Distance     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
VC Link Init      .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked L_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked G_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Disabled E_Port   .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
ISL R_RDY Mode    .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
RSCN Suppressed   .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Persistent Disable.. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
NPIV capability   ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON

Ports of Slot 0   16 17 18 19   20 21 22 23   24 25 26 27   28 29 30 31
-----------------+--+--+--+--+----+--+--+--+----+--+--+--+----+--+--+--
Speed             AN AN AN AN   AN AN AN AN   AN AN AN AN   AN AN AN AN
Trunk Port        ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
Long Distance     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
VC Link Init      .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked L_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked G_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Disabled E_Port   .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
```

```
ISL R_RDY Mode    .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
RSCN Suppressed   .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Persistent Disable.. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
NPIV capability   ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON

                  where AN:AutoNegotiate, ..:OFF, ??:INVALID.
                        LM:L0.5
```

The previous example shows no ports configured across the RSCN Suppressed line. In Example 1-5 we can see that it is enabled on ports 4 to 7.

Example 1-5 portcfg

```
ITSO_2005_B32:admin> portcfg rscnsupr 4-7 --enable
ITSO_2005_B32:admin> portcfgshow
Ports of Slot 0    0  1  2  3    4  5  6  7    8  9 10 11   12 13 14 15
-----------------+--+--+--+--+----+--+--+--+----+--+--+--+----+--+--+--
Speed             AN AN AN AN   AN AN AN AN   AN AN AN AN   AN AN AN AN
Trunk Port        ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
Long Distance     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
VC Link Init      .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked L_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked G_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Disabled E_Port   .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
ISL R_RDY Mode    .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
RSCN Suppressed   .. .. .. ..   ON ON ON ON   .. .. .. ..   .. .. .. ..
Persistent Disable.. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
NPIV capability   ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON

Ports of Slot 0   16 17 18 19   20 21 22 23   24 25 26 27   28 29 30 31
-----------------+--+--+--+--+----+--+--+--+----+--+--+--+----+--+--+--
Speed             AN AN AN AN   AN AN AN AN   AN AN AN AN   AN AN AN AN
Trunk Port        ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
Long Distance     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
VC Link Init      .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked L_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked G_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Disabled E_Port   .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
ISL R_RDY Mode    .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
RSCN Suppressed   .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Persistent Disable.. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
NPIV capability   ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON

                  where AN:AutoNegotiate, ..:OFF, ??:INVALID.
                        LM:L0.5
```

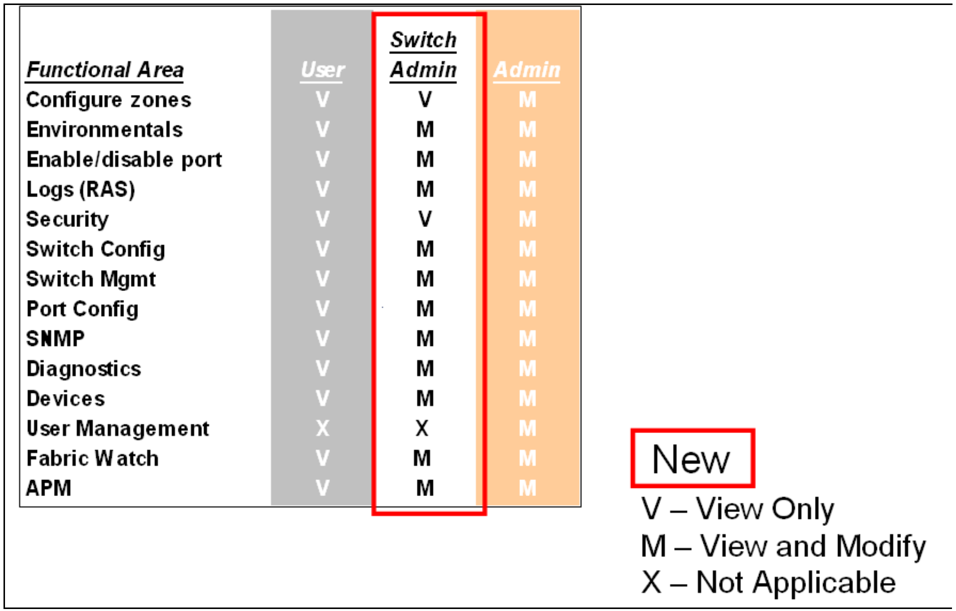
Any device connected to a switch running pre-FOS v5.0.x still receives RSCNs from an RSCN suppressed port.

Role-Based Access Control (RBAC)

With Role-Based Access Control, we are in a position to create users on a switch or director that only have access to predefined functions or roles. By default, these b-type switches come with 4 predefined userids: root; factory; admin; user. These userids have fixed roles, that of: root, factory, admin, and user. We can create multiple new users and assign them to these existing four roles, or to a new role called “switchadmin”. For example, we can create userids for Tom, John, Jane, Paulo; assign Paulo and Jane into the admin role, and therefore they have the same access as the default “admin” userid, and assign John and Tom into the user role.

The “switchadmin” role has most of the existing permissions of the traditional “admin” role, but cannot create/change fabric security policies; it cannot create/change fabric zoning policies, and cannot create/manage users.

The **`userconfig`** command, available since FOS 4.4, enables us to add new users and assign them to the existing default roles, or to the new role (available in FOS 5.0.x) “switchadmin”. Figure 1-9 shows all available functions for each role.



Functional Area	User	Switch Admin	Admin
Configure zones	V	V	M
Environmentals	V	M	M
Enable/disable port	V	M	M
Logs (RAS)	V	M	M
Security	V	V	M
Switch Config	V	M	M
Switch Mgmt	V	M	M
Port Config	V	M	M
SNMP	V	M	M
Diagnostics	V	M	M
Devices	V	M	M
User Management	X	X	M
Fabric Watch	V	M	M
APM	V	M	M

V – View Only
M – View and Modify
X – Not Applicable

Figure 1-9 Role access available with Switchadmin role

1.4 Management tools

Users can access internal management functions using standard host-based Simple Network Management Protocol (SNMP) software or Web browsers. They can access these functions using network connectivity through the Ethernet port or using in-band Internet Protocol (IP) through the Fibre Channel ports. The management functions of the switch allow a user to monitor frame throughput, error statistics, fabric topology, fans, cooling, media type, port status, IDs, and other information to aid in system debugging and performance analysis.

1.4.1 WebTools

WebTools is an intuitive graphical user interface (GUI) that allows network managers to monitor and manage SAN fabrics consisting of switches using a Java™-capable Web browser from standard desktop workstations. By entering the network address of any switch in the fabric, the built-in Web server automatically provides a full view of the switch fabric. From that switch, the administrator can monitor the status and perform administration and configuration actions on any switch in the SAN.

WebTools can manage the switches in the fabric either using in-band Fibre Channel connections or out-of-band Ethernet connections.

To increase SAN management security, WebTools can operate over a secure browser using the Secure Sockets Layer (SSL) protocol. This protocol provides data encryption, server authentication, message integrity, and optional client authentication for TCP/IP connections. Because SSL is built into all major browsers and Web servers, installing a digital certificate activates the SSL capabilities.

All the current functionality available in WebTools is discussed within 1.7, “Implementation” on page 41.

1.4.2 Fabric Watch

Fabric Watch monitors key fabric and switch elements, making it easy to quickly identify and escalate potential problems. It monitors each element for out-of-boundary values, or counters, and provides notification when any exceed the defined boundaries. Fabric Watch can configure elements, such as error status, and performance counters within a switch, and how they are monitored.

If an element exceeds the specified threshold or trigger value, Fabric Watch issues an alert. This can be in the form of writing to the event log, logging to the port log, issuing an SNMP trap, or sending an e-mail (or a combination of any of these).

The Fabric Watch feature monitors the performance and status of the IBM TotalStorage SAN Switch, and can alert SAN managers when problems arise. The real-time alerts from Fabric Watch software help SAN managers solve problems before they become costly failures. SAN managers can configure Fabric Watch software to monitor any of the following occurrences:

- Fabric events (such as topology re-configurations and zone changes)
- Physical switch conditions (such as fans, power supplies, and temperature)
- Port behavior (such as state changes, errors, and performance)
- Physical SFP conditions (for switches equipped with SMART SFPs)

Range monitoring

With Fabric Watch, each switch continuously monitors error and performance counters against a set of defined ranges. This, and other information specific to each monitored element, is made available by Fabric Watch for viewing, and in some cases, modification. This set of information about each element is called a threshold, and the upper and lower limits of the defined ranges are called *boundaries*.

If conditions break out of acceptable ranges, an *event* is considered to have occurred, and one or more *alarms* (reporting mechanisms) are generated if configured for the relevant threshold. There are three types of alarms:

- SNMP trap
- Entry in the switch event log
- Locking of the port log to preserve the relevant information

Element categories

Fabric Watch elements include any component of the fabric or switch that Fabric Watch software monitors. To monitor elements, Fabric Watch software categorizes them into areas, and groups these areas into classes.

Classes

Classes (also known as agents) are high-level categories of elements. Fabric Watch software monitors elements that compose the following classes:

- Fabric
- Environment
- Port (includes E_Port, Optical F/FL_Port, Copper F/FL_Port)
- SPF
- Performance Monitor (AL_PA, End-to-End, Filter)

Areas

Areas are the behaviors that Fabric Watch software monitors. Table 1-7 lists all Fabric Watch classes, the areas within those classes, and a description of each area.

Table 1-7 Fabric Watch Classes and Areas

Class	Area	Area description
Fabric	E_Ports downs	Monitors E_Port status
	Fabric Reconfigure	Monitors changes to the fabric configuration
	Domain ID Changes	Monitors forcible domain ID changes
	Segmentation Changes	Monitors segmentation changes
	Zone Changes	Monitors changes to currently enabled zoning configurations
	Fabric <-> QL	Monitors changes to QuickLoop
	Fabric logins	Monitors the number of host device fabric logins (FLOGI)
	SFP State Change	Monitors insertion/removal of smart SFP
Environmental	Temperature	Monitors switch temperature in degrees Celsius
	Fan	Monitors switch fan speed in RPMs
Port	Link Loss	Monitors the link failure rate of each port; tracks the number of link failures per configured time interval
	Sync Loss	Monitors the number of synchronization loss errors per configured time interval
	Signal Loss	Monitors the number of signal loss errors per configured time interval
	Protocol Error	Monitors the number of protocol errors per configured time interval
	Invalid Words	Monitors the number of invalid words transmitted (from a device to a port) per configured time interval
	Invalid CRCs	Monitors the number of CRC errors per configured time interval
	Rx Performance	Monitors receive rate in KB/sec
	Tx Performance	Monitors transmit rate in KB/sec
	State Changes	Monitors state changes

Class	Area	Area description
SFP	Temperature	Monitors SFP temperature in degrees Celsius
	Rx Power	Monitors SFP receiver power in uWatts
	Tx Power	Monitors SFP transmitter power in uWatts
	Current	Monitors SFP current in mAmps
	Voltage	Monitors SFP power in mVolts
Performance Monitor	CRC Errors	Monitors the number of CRC errors that occur (for AL_PA or for a SiD-DiD pair) per configured time interval (in seconds)
	FCW Received	Monitors receive rate of a SiD-DiD pair in KB per second
	FCW Transmitted	Monitors transmit rate of a SiD-DiD pair in KB per second
	Custom Filter Counter	Monitors the filter-based counter that the user defines

1.4.3 SNMP

Simple Network Management Protocol (SNMP) allows network devices to be monitored, controlled, and configured remotely from a network management station running a network manager program.

SNMP agent code in the network device allows management by transferring data that is specified by a Management Information Base (MIB).

The switch agent supports the following features:

- SNMPv1 manager
- SNMPv3 in FOS 4.4 compatible with older SNMPv1
- Command-line utilities to provide access to and command the agent
- MIB-II system group, interface group, and SNMP group
- Fabric-element MIB
- IBM-specific MIBs
- Standard generic traps
- IBM-specific traps

1.4.4 Fabric Manager

Fabric Manager is an application that provides a graphical interface allowing you to monitor and manage multiple fabrics from a standard workstation. Fabric Manager can be used to manage fabric wide settings such as zoning and also manage settings at an individual switch level.

Fabric Manager provides high-level summary information about all switches in a fabric, automatically launching the WebTools interface when more detailed information is required. The launching of WebTools is transparent, providing a seamless user interface. In addition to the ability to view switches as groups, Fabric Manager provides improved performance over WebTools alone.

Fabric Manager installs on a workstation, and can be used to manage IBM TotalStorage SAN Switches that have Fabric OS version 2.2 or later and the WebTools license installed. All the switches in the fabric are represented in the main window of Fabric Manager, but only those with a WebTools license can be managed through Fabric Manager.

New to FM 5.x

With the introduction of Fabric Manager 5.1, all previous functionality is still supported. We introduce a wealth of new tools and functionality to further reduce the complexity of managing and maintaining a SAN infrastructure. FOS 5.0 provided support for the recent SAN-256B (2109-M48) director and the SAN-16B (2005-B16) switch. The most significant change in FOS 5.1 is the support for the new SAN18B-R (2005-R18) and the FC Routing Blade for the SAN256B-2.

Single signon to WebTools

FM 5.0 introduced an auto-authentication with all WebTools sessions using previously gathered login/passwords. If the login details have been entered previously, they are now stored in the FM repository for further use, otherwise the administrator is prompted for this information as normal. To support this functionality, attached switches must be running FOS 4.1 or greater. However, this functionality is not yet available for the 2109-A16 router as it runs the XPath Operating System.

Launch third party management applications

FM 5.x can now spawn external management application from within its own menu system, for example, Tivoli® SAN Manager.

Integrated FTP server and firmware repository

One of the most significant changes to FM is the integration of a firmware repository and a built-in FTP server allowing all switches and directors to connect directly to FM to retrieve a newer version of FOS. The FTP server is from Apache and supports passive mode and supports up to 10 simultaneous connections. It is not necessary to use this built-in FTP server, external servers are still supported.

As the name suggests, the firmware repository allows you to store multiple versions on FOS in a manageable format in the repository. If you have a fabric containing three different types of b-type hardware, it would not be uncommon to have two or three different versions of FOS for each architecture. All these versions can be stored and easily accessed via the firmware repository.

Device diagnostics wizard

This tool allows you to perform diagnostic checks on a device that might have a communication problem within your fabric. It can also check for communication problems between devices in separate fabrics that are connected together via a b-type SAN router. The GUI displays a list of devices, where we select any two. From here it performs a list of checks and provides you with a report of its findings. The report covers areas like zoning; physical device connectivity; LSAN zoning (for routed devices) and security policy checks.

Excel reports

FM 5.0 provides you with a GUI interface allowing the execution of fabric summary reports (switches per fabric, health of switches, port utilization, and so on) without the necessity of using the Fabric Manager client, but these reports are also available from the client itself. Be aware that Microsoft Excel® needs to be installed on the machine from which you initiate the report.

Physical inventory of the SAN

FM provides a feature to collect and store all physical inventory data in the Fabric Manager repository at an interval of once a day. Optionally, you can manually initiate the SAN data collection on a selected fabric or fabrics from the Action menu option.

FM provides a report that allows you to collect an entire physical inventory of the SAN for analysis. This report focuses on the physical components with sufficient selection and query facilities so that the user can target items of interest. For example, a field technician can run a report to extract all power supply and fan information for all switches in the fabric, or query solely to obtain any failing fan or power supply.

Replicate AAA configuration to other switches

The Replicate AAA Configurations Wizard replicates an AAA configuration to a fabric or a user selected group of switches. You can set up an AAA configuration and a Radius configuration on one switch via WebTools or the CLI. Then you can replicate that setting to one or more switches using this Wizard.

Advantages of Fabric Manager

Fabric Manager is a complete SAN management tool, with the following advantages:

- Provides a highly scalable Java-based application that manages multiple switches and multiple fabrics in real-time.
- Assists you with configuring, monitoring, dynamic provisioning, and daily management of SANs.
- Lowers the cost of SAN ownership by intuitively facilitating SAN management tasks.
- Saves time by enabling the global integration and running of processes across multiple fabrics through its single-point SAN management platform.
- Allows more effective management by providing rapid access to critical SAN information across both Fabric OS SANs and enhanced Fabric OS SANs.

Capabilities

With WebTools, Fabric Manager provides the following information and capabilities:

- Configures and manages the fabric on multiple efficient levels.
- Intelligently groups multiple SAN objects and SAN management functions to provide ease and time-efficiency in administering tasks.
- Identifies, isolates, and manages SAN events across multiple switches and fabrics.
- Provides drill-down capability to individual SAN components through tightly coupled WebTools and Fabric Watch integration.
- Discovers all SAN components and views the real-time state of all fabrics.
- Provides multi-fabric administration of secure Fabric OS SANs through a single encrypted console.
- Implements scalable SAN management tasks through functionality and tools that intelligently span eight fabrics and 200 switches.
- Monitors ISLs.
- Manages switch licenses.
- Enables you to take a snapshot of your ISL design so that you can monitor any changes.

Concepts

In the following sections we describe the concepts that are supported by Fabric Manager.

Logical groups

We can create logical groups to monitor the status of their component switches and propagate actions over the chosen group of switches. We can also use this feature to quickly determine the status of a large number of switches without looking through each one. A logical group differs from a physical group in that it does not necessarily represent a physically grouped set of switches.

Local files

Fabric Manager saves groups and other information to local files. Fabric Manager stores these files in our home directory. Log files are under the following directory:

```
user home/Fabric Manager/log
```

Import/export

Logical groups and other configuration information can be saved to local files and shared between hosts through the Import and Export options. Additionally, configuration information can be imported from files.

Security

> **Note:** This feature is not available without Advanced Security.

Security is implemented on a policy basis. Advanced Security enables sensitive operations to be restricted to a few trusted switches. It allows you to designate a small number of switches (known as Fabric Configuration Servers) for fabric-wide management operations. Individual switches are still be accessed for local configuration. It is possible to configure Advanced Security in such a way that Fabric Manager is unable to access most of the switches. In this case Fabric Manager can only be used in a reduced mode without most monitoring features and lacking many of the administration launch points.

1.5 Licensing

We discuss the licensing options available in the topics that follow.

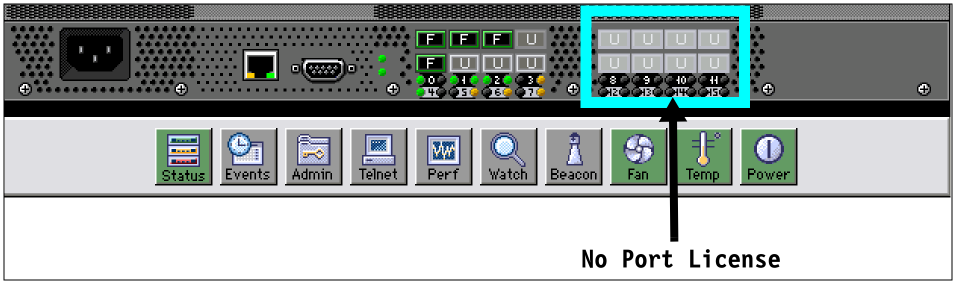
1.5.1 Ports on Demand

The Ports on Demand (POD) feature was introduced with the SAN32B enabling you to “Pay as you grow” your fabric. Dependent upon the switch type, we are able to grow our initial port count in blocks of 4, 8 or 16 ports per license. As a rule of thumb, each switch with the POD capability comes shipped with 50% of the ports configured. POD upgrades are available in 25% increments. For example:

- SAN16B (16 physical ports) ships with 8 ports initially activated. POD is in increments of 4 ports.
- SAN32B (32 physical ports) ships with 16 ports activated and with a POD license can be upgraded in 8-port or 16-port block(s).
- SAN64B (64 physical ports) ships with 32 ports activated and with a POD license can be upgraded in 16-port block(s).

Enabling these licenses via WebTools, or the CLI using **`licenseAdd`** and **`portEnable`** are both non-disruptive. If we remove a POD license by mistake, the affected ports continue to operate until the switch is disabled or rebooted.

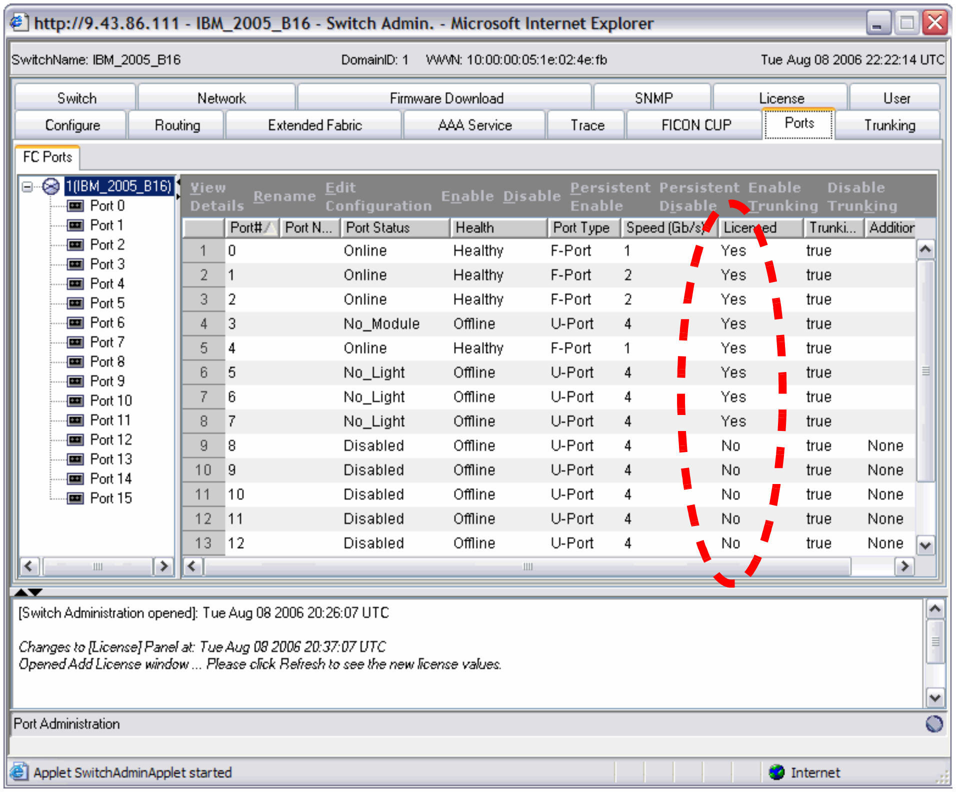
Within the WebTools GUI, unlicensed ports are “greyed out”, as shown here in Figure 1-10. These ports can still be configured but cannot be activated.



No Port License

Figure 1-10 WebTools showing unlicensed ports

The WebTools GUI also supports a new column within the ports administration window (see Figure 1-11 on page 37), which enables you to verify which ports are licensed and which are not.



Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Ports
Trunking
FC Ports
1(IBM_2005_B16)
Port 0
Port 1
Port 2
Port 3
Port 4
Port 5
Port 6
Port 7
Port 8
Port 9
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15
View Details
Rename
Edit Configuration
Enable
Disable
Persistent Enable
Persistent Disable
Enable Trunking
Disable Trunking
Port Administration
Internet

http://9.43.86.111 - IBM_2005_B16 - Switch Admin. - Microsoft Internet Explorer

SwitchName: IBM_2005_B16 DomainID: 1 WWN: 10:00:00:05:1e:02:4e:fb Tue Aug 08 2006 22:22:14 UTC

	Port#	Port N...	Port Status	Health	Port Type	Speed (Gb/s)	Licensed	Trunki...	Addition
1	0		Online	Healthy	F-Port	1	Yes	true	
2	1		Online	Healthy	F-Port	2	Yes	true	
3	2		Online	Healthy	F-Port	2	Yes	true	
4	3		No_Module	Offline	U-Port	4	Yes	true	
5	4		Online	Healthy	F-Port	1	Yes	true	
6	5		No_Light	Offline	U-Port	4	Yes	true	
7	6		No_Light	Offline	U-Port	4	Yes	true	
8	7		No_Light	Offline	U-Port	4	Yes	true	
9	8		Disabled	Offline	U-Port	4	No	true	None
10	9		Disabled	Offline	U-Port	4	No	true	None
11	10		Disabled	Offline	U-Port	4	No	true	None
12	11		Disabled	Offline	U-Port	4	No	true	None
13	12		Disabled	Offline	U-Port	4	No	true	None

```
[Switch Administration opened]: Tue Aug 08 2006 20:26:07 UTC

Changes to [License] Panel at: Tue Aug 08 2006 20:37:07 UTC
Opened Add License window ... Please click Refresh to see the new license values.
```

Applet SwitchAdminApplet started

Figure 1-11 WebTools showing licensed ports

1.5.2 Extended Fabric

Extended Fabric Activation extends SAN fabrics beyond the Fibre Channel standard of 10 km by optimizing the internal switch buffers to maintain performance on ISLs at distances up to 500 km.

1.5.3 Performance Monitoring

Performance Monitoring is a licensed feature that provides error and performance information to manage your storage environment. We have three main types of monitoring:

- **Arbitrated Loop Physical Address (AL_PA) monitoring:** This provides information regarding the number of CRC errors.

- **End-to-end monitoring:** This provides information regarding a configured source identifier (SID) to destination identifier (DID) pair. Information includes the number of CRC errors for frames with the SID-DID pair, Fibre Channel words transmitted from the port for the SID-DID pair, and Fibre Channel words received for the port for the SID-DID pair.
- **Filter-based monitoring:** This provides error information with a customer-determined threshold.

1.5.4 ISL Trunking

ISL Trunking enables Fibre Channel packets to be efficiently distributed across multiple Inter-Switch connections (links) between two SAN b-type fabric switches, while preserving in-order delivery. Both SAN b-type fabric switches must have ISL Trunking activated.

1.6 Security

In the following topics we discuss security features.

1.6.1 Advanced Security / Secure Fabric OS

Secure Fabric OS (SFOS) is a licensed product that provides customizable security restrictions through local and remote management channels on a b-type fabric. It does this and more using the following functionality:

- Fabric Configuration Server (FCS), providing centralized management of fabric-wide configurations and policies.
- Management Access Control (MAC), providing additional layers of granularity when enforcing what devices can access SAN switches by way of which applications.
- Secure Management Channels (SMC), providing a more secure method for running management applications that use encrypted passwords and certificates for authentication.
- Switch Connection Control (SCC), improving switch-to-switch authentication by allowing the use of digital certificates as well as locking down which ports can become E_Ports.
- Device Connection Control (DCC), allowing secure switch to switch authentication (per their WWNs) from a specific port or group of ports.

However, before implementing an SFOS environment, some minimum requirements have to be met, as shown in Table 1-8.

Table 1-8 Secure Fabric OS - supported switches and fabrics

Fabric OS version	Supported hardware
V2.6.2	2109-S08, 2109-S16
V3.2.0	3534-F08, 2109-F16
V4.4.0	2109-F32, 2109-M12, 2109-M14, 2005-B32
V5.0.1	2109-F32, 2109-M12, 2109-M14, 2109-M48,2005-H08, 2005-H16, 2005-B16, 2005-B32, 2005-B64

Note: V5.1.0 is supported for each of the SAN16B, SAN32B, SAN64B, and SAN256B switches.

Fabric Configuration Server

FCS tackles the issue of centralized management by creating a multi-tiered switch configuration infrastructure. This provides a framework for change management activities as well as the ability to mitigate security risks through fabric lockdown.

The practicalities of FCS are that each switch in a fabric requires grouping into into three logical areas:

- Primary FCS Switch: A single powerful switch that is the sole authority for all read/write access to fabric wide operations. Commonly this would be a core switch which has the best controlled physical security and is the most robust switch in the fabric.
- Backup FCS switches: One or more switches that are able to take Primary FCS control if the original Primary FCS switch becomes unavailable. The backup FCS switch cannot make any changes to the fabric unless it has become the primary FCS.
- Non-FCS switches: All remaining switches in the fabric. None of these switches have the power to make any fabric wide changes.

Management Access Control (MAC)

This functionality enables SAN administrators to choose how to manage their SAN. This is implemented using three categories:

- Remote access limitation: Look up the remote accessing device IP address in the appropriate Security Policy to see whether access is allowed.
- Port-based access: Look up the WWN of the accessing device in the appropriate security policy to see whether access is valid.

- Physical Access Connections: Look up the WWN of the connecting switch in the appropriate security policy to see whether fabric access is valid.

Secure Management Channels (SMC)

SFOS provides secure channels for management via provided policies. These include: Fabric Manager, WebTools and standard SNMP applications.

Secure Fabric OS policies are also available for telnet (includes sectelnet and Secure Shell), SNMP, management server, HTTP, and API.

After a digital certificate has been installed on the switch, Fabric OS v3.2.0, v4.4.0, v5.0.1, and v5.1.0 encrypt sectelnet, API, and HTTP passwords automatically, regardless of whether Secure Fabric OS is enabled.

Secure Shell (SSH)

Fabric OS v4.4.0 and v5.0.1 support SSH, enabling fully encrypted telnet sessions and is configured within the Telnet Policy of SFOS. Using SSH does not require a digital certificate on the switch, nor does it require the purchase of the Advanced Security product.

sectelnet

The sectelnet client is a secure form of telnet that encrypts passwords only. It is configured within the Telnet policy of SFOS. Fabric OS v4.4.0, v5.0.1 and v5.1.0 include the sectelnet server.

Telnet

Standard telnet is not available when secure mode is enabled. The telnet button in WebTools is also disabled.

Switch Connection Control (SCC)

Switch-to-switch authentication is supported via Public Key Infrastructure (PKI) or Diffie-Hellman Challenge-Handshake Authentication Protocol (DH-CHAP).

Public Key Infrastructure

Both PKI-based digital certificates and switch WWNs, along with SLAP or FCAP, can be used to prevent unauthorized switch access to the fabric.

Diffie-Hellman Challenge-Handshake Authentication Protocol

DH-CHAP shared secrets can be used to provide switch-to-switch authentication and prevent the addition of unauthorized switches to the fabric. It requires a pair of shared secret keys — shared secrets — between each pair of switches authenticating with DH-CHAP.

Device Connection Control (DCC)

DCCs allow the SAN administrator to select which device WWNs can connect to which switch ports. By creating various unique policies using the name format, DCC_POLICY_xxx, administrators can lock down a fabric to varying degrees of granularity. To achieve extreme control (and high change management), the administrator can connect a fabric so that each switch port can connect to only a single WWN.

1.7 Implementation

In the topics that follow we show how to implement the b-type switches.

1.7.1 Initial setup

Prior to configuring the IBM TotalStorage SAN Switch, it must be physically mounted and connected to the appropriate electrical outlets. The amount of planning and preparation required for the installation is dependent upon the switch/director being installed. We recommend referring to the Brocade hardware reference guide for the model you plan to install, as this highlights the key aspects for your consideration. You must arrange for your IBM service representative to physically install the chassis or rack in the location you have planned.

After the switch is installed and powered on, it requires some initial configuration parameters to be set. All of the b-type switches require the same initial setup. The fundamental steps have not changed from the earlier switch models.

Switch Power On Sequence

When the switch is powered on or restarted, the following operations are performed; these take a minimum of three minutes to complete:

1. Early power-on self test (POST) diagnostics are run. POST is run before the FOS is started.
2. The FOS is initialized.
3. The hardware is initialized. The switch is reset, the internal addresses are assigned, the Ethernet port is initialized, the serial port is initialized, and the front panel is initialized.
4. A full POST is run.
5. The links are initialized. Receiver and transmitter negotiation is run to bring the connected ports online.

6. During the Fabric Login (FLOGI), link parameters are exchanged. This determines whether any ports are connected to other switches. If so, it negotiates who becomes the principal switch.
7. Domain addresses are assigned. After the principal switch is identified, port addresses are assigned. Each switch tries to keep the same domain ID that it used previously. Previous IDs are stored in the configuration Flash memory.
8. The routing table is constructed. After the addresses are assigned, the unicast routing tables are constructed.
9. Normal Nx_Port operation is enabled.

Figure 1-12 shows a chart describing the initialization sequence of a device when it is connected to an individual switch port.

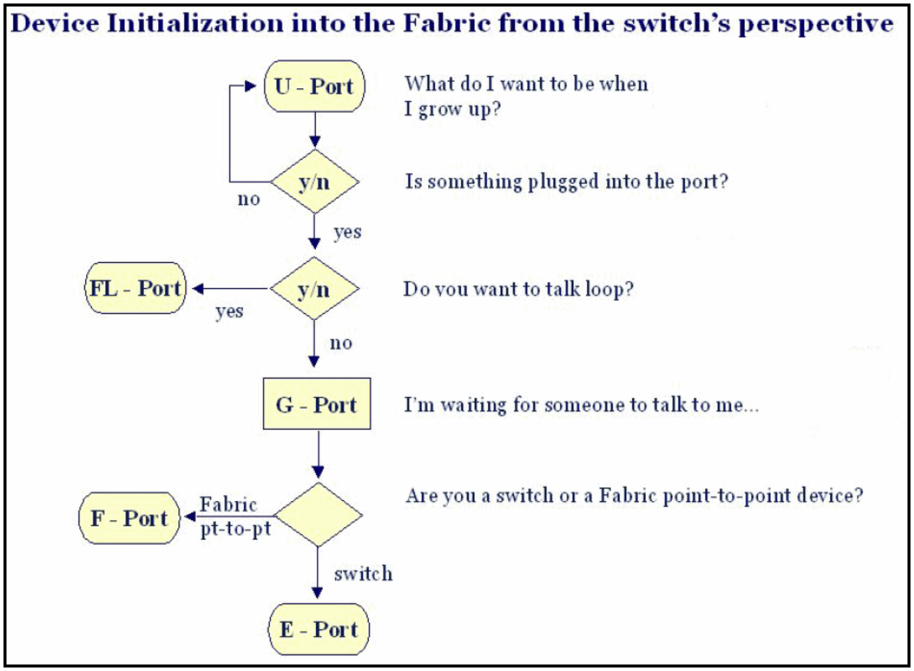

Device Initialization into the Fabric from the switch's perspective
U - Port
What do I want to be when I grow up?
y/n
no
Is something plugged into the port?
yes
FL - Port
yes
y/n
Do you want to talk loop?
no
G - Port
I'm waiting for someone to talk to me...
Are you a switch or a Fabric point-to-point device?
F - Port
Fabric pt-to-pt
switch
E - Port

Figure 1-12 Flow chart showing device initialization

When we have installed the switch or director into a rack, and it has successfully powered up through its POST tests, we have to perform some basic setup functions.

By connecting to the switch using a terminal emulator, we can see the switch POST tests as they progress.

Example 1-6 shows the startup of a SAN16B switch.

Example 1-6 SAN16B startup

```
The system is coming up, please wait...
Read board ID of 0x80 from addr 0x23
Read extended model ID of 0x19 from addr 0x22
Matched board/model ID to platform index 6

Read board ID of 0x80 from addr 0x23
Read extended model ID of 0x19 from addr 0x22
Matched board/model ID to platform index 6
Checking system RAM - press any key to stop test

Checking memory address: 00100000

System RAM test using Default POST RAM Test succeeded.

Press escape within 4 seconds to enter boot interface.
Booting "Fabric Operating System" image.
Entry point at 0x01000000 ...

Linux/PPC load:
BootROM command line: quiet
Uncompressing Linux...done.
Now booting the kernel
Attempting to find a root file system on hda1...
modprobe: modprobe: Can't open dependencies file
/lib/modules/2.4.19/modules.dep
 (No such file or directory)
INIT: version 2.78 booting
INIT: Entering runlevel: 3

INITCP: CPLD Vers: 0x90 Image ID: 0x1c
uptime: 2606; sysc_qid: 0


Fabric OS (IBM_2005_B16)


IBM_2005_B16 console login:
2006/07/31-21:20:04, [HAM-1004], 38,, INFO, IBM_2005_B16, Processor rebooted -
Unknown
SNMP Research SNMP Agent Resident Module Version 15.3.1.4
Copyright 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999,
2000, 2001 SNMP Research, Inc.
sysctrld: all services Standby
sysctrld: all services Active
POST1: Started running Mon Jul 31 21:20:14 GMT 2006
```

```
POST1: Test #1 - Running turboramtest
POST1: Test #2 - Running portregtest
POST1: Script PASSED with exit status of 0 Mon Jul 31 21:20:15 GMT 2006 took
(0:
0:1)
POST2: Started running Mon Jul 31 21:20:16 GMT 2006
POST2: Test #1 - Running portloopbacktest (TXRX INTERNAL)
POST2: Test #2 - Running minicycle (TXRX INTERNAL)
POST2: Running diagshow
POST2: Script PASSED with exit status of 0 Mon Jul 31 21:20:31 GMT 2006 took
(0:
0:15)
2006/07/31-21:20:32, [BL-1000], 39,, INFO, IBM_2Enabling switch...
005_B16, Initializing Ports...
2006/07/31-21:20:32, [BL-1001], 40,, INFO, IBM_2005_B16, Port Initialization
Completed



Fabric OS (IBM_2005_B16)


IBM_2005_B16 console login:
```

In order to view the console login prompt, you must press the Enter key. It is useful to be aware of the standard boot up sequence for your switch so that, should a problem arise, it is easy to distinguish between standard and abnormal behavior.

1.7.2 The command line interface

To access the management interfaces of a switch or director from a remote workstation on a network, we have to set the IP address, subnetmask, and gateway address for the switch, or for each of the CPs and the chassis in a SAN256B. These settings can be modified using the **ipAddrSet** command.

- We show the steps to perform this in “SAN256B configuration procedure” on page 49.

  The default IP address and subnet mask for the SAN16B, SAN32B, and SAN64B switches are as follows:

  – 10.77.77.77 255.255.255.0

  The default IP addresses, subnet mask, and switch names for a SAN256B are as follows. This IP address correspond to “sw0”, the chassis:

  – 10.77.77.77 255.255.255.0 sw0

The SAN256B also has native IP addresses to access each CP card. The default native IP addresses, subnet masks, and hostnames are as follows:

  - 10.77.77.75 255.255.255.0 CP0 (the CP Card in slot 5 at the time of configuration)
  - 10.77.77.74 255.255.255.0 CP1 (the CP Card in slot 6 at the time of configuration)

- **Domain ID:** For switches to be connected together within a fabric, each switch must have different domain IDs. The default domain ID for a switch is 1. If two switches are connected via an ISL after initialization is complete, they will segment due to both switches having the same domain ID. Domain IDs can be modified using the **`configure`** command. We show an example of how to do this in 1.7.3, “Connecting to the switch” on page 52.
- **Switch names:** Setting a switch name to identify different switches within a site is recommended. This is very helpful in easily identifying a switch that you are connected to. By using the **`switchname`** command, you can assign your own switch names, which can be up to 15 characters long, must begin with an alpha character, and can include alpha, numeric, and underscore characters.

Following are the steps we took to configure the above settings and connect our switch for use in a network and fabric. We also include the extra steps required to configure a SAN256B.

The time required to accomplish this is approximately 15 minutes. The following items are required:

- 2005 or 2109 physically installed and connected to a power source
- A workstation that has a terminal emulator application (we used HyperTerminal)
- The serial cable provided with the switch, for connecting the switch to the workstation. If your workstation does not have a 9 pin serial port, you might require an adapter; we used a USB Serial Adapter to connect.
- An unused IP address (SAN256B requires three IP addresses) plus gateway IP address and subnet mask
- Ethernet cable for connecting the switch to the workstation or to a network containing the workstation
- SWL or LWL SFPs and fiber optic cables as required

Note: We recommend that you do not connect the switch to your LAN until the IP settings are properly configured and do not conflict with any other devices in your network.

It is important to leave at least 3.28 ft. (1 m) of slack for each port cable. This provides room to remove and replace the switch, allows for inadvertent movement of the rack, and helps prevent the cables from being bent to less than the minimum bend radius.

We recommend that you use Velcro straps to secure and organize fibre optic cables. Do not use tie wraps on fiber optic cables as these are easily overtightened and can damage the optic fibers.

Setting the IP address using the serial port

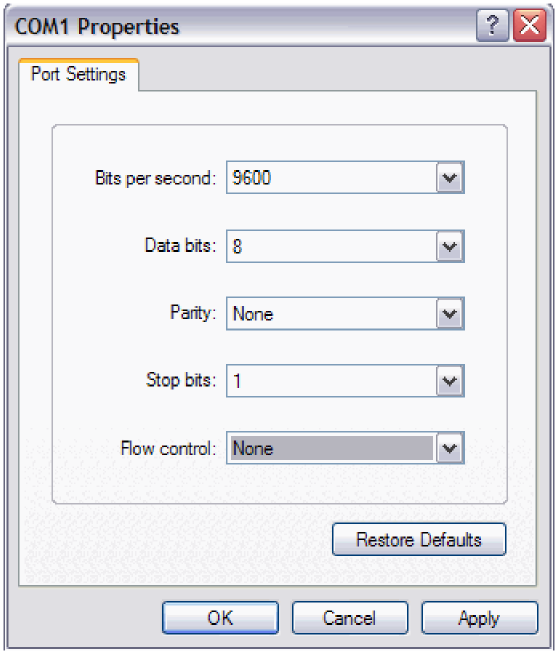
Below are the steps we used to set the IP address using the serial port on an IBM SAN16B-2. The procedure is the same for all b-type switches except for the IBM SAN256B. We show the steps for a SAN256B (M48) in “SAN256B configuration procedure” on page 49.

1. Remove the shipping plug from the serial port and insert the serial cable provided with the switch.
2. Connect the other end of the serial cable to an RS-232 serial port on the workstation. If you do not have a male DB-9 serial port connector on your workstation, you must convert the serial cable in order to communicate. We used a USB serial adapter.

   > **Tip:** The serial cable shipped with the switch is a straight-through cable, not a cross-over cable. We recommend labeling the cable as such to minimize confusion at a later date.

3. Verify that the switch is on and initialization has completed. This can be verified by confirming that both the system and power status LEDs are both on and green.
4. Disable any serial communication programs running on the workstation, such as PDA synchronization.
5. Open a terminal emulator application (such as HyperTerminal on a PC, or TERM in a UNIX environment), and configure as follows:
   a. In a Microsoft Windows environment, adjust the following parameters and values if necessary; see Figure 1-13.
      - Bits per second: 9600
      - Databits: 8
      - Parity: None
      - Stop bits: 1
      - Flow control: None

Figure 1-13 Shows the HyperTerm COM1 properties window.



Bits per second: 9600

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

Figure 1-13 HyperTerm COM1 properties window

b. In a UNIX environment, enter the following string at the prompt:

```
tip /dev/ttyb -9600
```

From the terminal emulator application, logon to the switch through the serial connection. The default administrative logon is **`admin`** and the default password is **`password`**. If you have just powered up the switch, you might have to press Enter to display the login prompt following the `Port Initialization Completed` message. When logging into a new switch you are requested to change the password. In order to skip this type `ctrl-c`, you are prompted to change the password again at your next login. If you choose to change the password at this stage, you are prompted to change the password for each of the generic user accounts: root, factory, admin and user. When all of the password authentication tokens are updated, they are saved to stable storage. We recommend changing the password prior to connecting the switch to your network.

6. Enter the following command at the prompt:

```
ipAddrSet
```

7. Enter the following information at the corresponding prompts, listed below:

`Ethernet IP Address [10.77.77.77]:` *`Enter new ethernet IP address`*

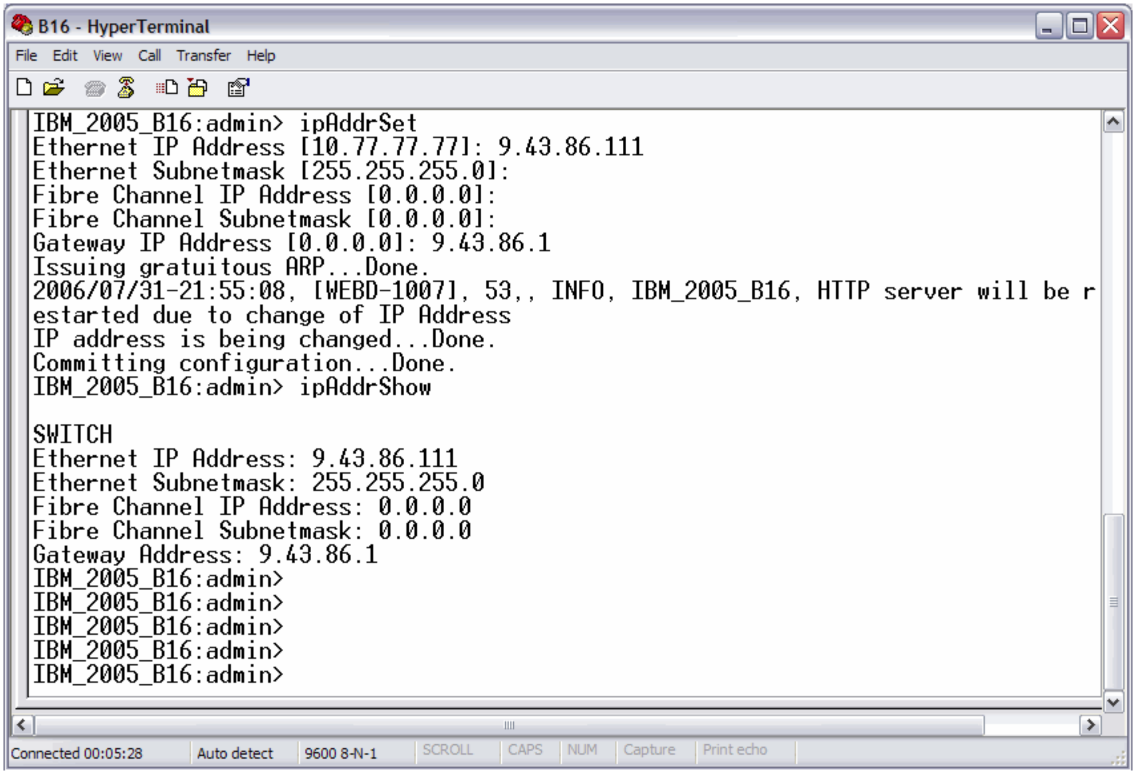
Ethernet Subnetmask [255.255.255.0]: *Enter new ethernet subnetmask*
Fibre Channel IP Address [0.0.0.0]: *Enter new Fibre Channel IP address if desired*
Fibre Channel Subnet Mask [0.0.0.0]: *Enter new Fibre Channel subnet mask if desired*
Gateway Address [0.0.0.0]: *Enter new gateway address*

8. We can verify that the address was correctly set by entering this command: **`ipAddrShow`**
9. After verifying that the IP address is correct, remove the serial cable, and replace the shipping plug in the serial port.

> **Note:** The serial port is intended only for use during the initial setting of the IP address and for service purposes.

10. Record the IP address for future reference.

Figure 1-14 details the Ethernet IP address configuration.



```
IBM_2005_B16:admin> ipAddrSet
Ethernet IP Address [10.77.77.77]: 9.43.86.111
Ethernet Subnetmask [255.255.255.0]:
Fibre Channel IP Address [0.0.0.0]:
Fibre Channel Subnetmask [0.0.0.0]:
Gateway IP Address [0.0.0.0]: 9.43.86.1
Issuing gratuitous ARP...Done.
2006/07/31-21:55:08, [WEBD-1007], 53,, INFO, IBM_2005_B16, HTTP server will be r
estarted due to change of IP Address
IP address is being changed...Done.
Committing configuration...Done.
IBM_2005_B16:admin> ipAddrShow

SWITCH
Ethernet IP Address: 9.43.86.111
Ethernet Subnetmask: 255.255.255.0
Fibre Channel IP Address: 0.0.0.0
Fibre Channel Subnetmask: 0.0.0.0
Gateway Address: 9.43.86.1
IBM_2005_B16:admin>
IBM_2005_B16:admin>
IBM_2005_B16:admin>
IBM_2005_B16:admin>
IBM_2005_B16:admin>
```

Figure 1-14 Set and display the Ethernet IP address

After the IP address is set, we are able to connect the switch to the workstation computer by ethernet cable (this can be a direct cross-over connection or through a network) by following these steps:

1. Remove the shipping cover from the ethernet port.
2. Insert one end of an ethernet cable in the ethernet port.
3. Connect the other end of the ethernet cable to the workstation or to an ethernet network containing the workstation.

   Note: The switch can now be accessed remotely, through Telnet or WebTools. As a result, it is important to ensure that the switch is not being modified simultaneously from any other connections during the remaining steps.

SAN256B configuration procedure

The initial communication to a SAN256B requires a serial connection. Follow the steps below to establish a serial connection and log in to the director:

1. Verify that the director is powered on and that POST is complete by verifying that all power LED indicators on the port blades and CP blades are displaying a steady green light.
2. Use the serial cable provided with the director to connect the console port on the active CP blade to a computer workstation.

   Note: The console port is the second serial port from the top of the CP blade. The active CP blade is indicated by an illuminated (blue) LED. The LED on the standby CP blade should be off (not illuminated). This console port is intended primarily for use during the initial setting of the IP address and for service purposes. If necessary, the adapter on the end of the serial cable can be removed to allow for an RJ-45 serial connection.

3. Access the director using a terminal emulator application (such as HyperTerminal on Windows 95, 2000, or NT, or TERM in a UNIX environment).
4. Disable any serial communication programs running on the workstation (such as synchronization programs).
5. Open the terminal emulator application and configure as follows:
   - Bits per second: 9600
   - Databits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None

For most UNIX systems, type the following string at the prompt:

```
tip /dev/ttyb -9600
```

When the terminal emulator application stops reporting information, press Enter. You receive the following login prompt:

```
swDir Console Login:
```

6. Log in to the director as admin. The default password is ***password***.

> **Note:** At the initial login, the user is prompted to enter new admin and user passwords.

7. Change the passwords. Passwords can be 8 to 40 characters long. They must begin with an alphabetic character. They can include numeric characters, the dot (.), and the underscore (_). Passwords are case-sensitive, and they are not displayed when you enter them on the command line. To skip modifying the password, press Ctrl- C.

```
CP0 Console login:admin
Password:
Please change your passwords now.
Use Control-C to exit or press 'Enter' key to proceed.
Password was not changed. Will prompt again at next login
until password is changed.
```

8. View the “Active CP” LED on the CP blades in slots 5 and 6 or enter the **`haShow`** command to verify which CP blade is active. The configuration can be modified only through a login session to the active CP blade.

```
swDir:admin> haShow
Local CP (Slot 6, CP1): Active
Remote CP (Slot 5, CP0): Standby
HA Enabled, Heartbeat Up, State Synchronized
```

Follow these steps to configure the IP addresses for the director and both CP blades (from the active CP blade):

1. Log in to the active CP as admin using the serial cable connection.
2. Set up the director IP address by entering the ipaddrset -sw 0 command at the prompt.

```
swDir:admin> ipAddrSet -sw 0
```

Enter the requested information at the prompts. Unlike the M12 and M14 model directors, the only valid configuration for the SAN256B is as a single domain (single logical switch), so you only have to specify the -sw 0 IP address. There is no -sw 1 on the SAN256B.

3. Set up the CP0 blade IP address by entering the **`ipaddrset -cp 0`** command at the prompt, including “0” for the CP blade in slot 5.

   ```
   swDir:admin> ipAddrSet -cp 0
   ```

   Enter the requested information at the prompts.

4. Set up the CP1 blade IP address by entering the **`ipaddrset -cp 1`** command at the prompt, including “1” for the CP blade in slot 6.

   ```
   swDir:admin> ipAddrSet -cp 1
   ```

   Enter the requested information at the prompts. The following is a sample IP configuration for the director (sw -0) and the two CP blades (cp0 and cp1).

   ```
   swDir:admin> ipaddrset -sw 0
   Ethernet IP Address [0.0.0.0]: 123.123.123.120
   Ethernet Subnetmask [0.0.0.0]: 123.123.123.123
   Fibre Channel IP Address [0.0.0.0]:
   Fibre Channel Subnetmask [0.0.0.0]:
   Issuing gratuitous ARP...Done.
   Committing configuration...Done.
   swDir:admin> ipaddrset -cp 0
   Host Name [cp0]:
   Ethernet IP Address [10.77.77.75]: 123.123.123.121
   Ethernet Subnetmask [0.0.0.0]: 123.123.123.123
   Gateway IP Address [0.0.0.0]: 123.123.123.124
   IP address is being changed...Done.
   Committing configuration...Done.
   swDir:admin> ipaddrset -cp 1
   Host Name [cp1]:
   Ethernet IP Address [10.77.77.74]: 123.123.123.122
   Ethernet Subnetmask [0.0.0.0]: 123.123.123.123
   Gateway IP Address [0.0.0.0]: 123.123.123.124
   IP address of remote CP is being changed...Done.
   Committing configuration...Done.
   ```

Note: Although the SAN256B Hardware reference manual suggests that a reboot is required when changing the IP address, this is not necessary. The IP address can be changed online without rebooting the director.

The terminal serial port can be used to monitor error messages through a serial connection. It is not recommended as a command interface during normal operations. If this port is not going to be in ongoing use, remove the serial cable and protect the port from dust by replacing the shipping cap. The SAN256B’s initial configuration is complete.

1.7.3 Connecting to the switch

After using a serial connection to configure the IP addresses for the director, you have to connect both the active and the standby CP blade to the local area network (LAN). We recommend connecting the CP blades to a private network/VLAN, because this provides additional security to your SAN as well as protection from network broadcast storms or other problems.

By establishing an Ethernet connection, you can complete director configuration using either the serial session or a Telnet session, or through the graphical management interfaces: WebTools and Fabric Manager. However, you must ensure that the director is not modified from other connections at the same time.

To establish an Ethernet connection to the director, follow these steps:

1. Remove the shipping plug from the Ethernet port on the active CP blade.
2. Insert one end of an Ethernet cable into the Ethernet port.
3. Connect the other end to an Ethernet 10/100 Base-T LAN.

   The director can now be accessed by remote connection using any of the available management tools, such as Telnet, WebTools, or Fabric Manager.
4. To complete any additional director configuration procedures through a Telnet session, log in to the director using Telnet with the admin login. The default password is *password*.

Important: When managing the SAN256B director, use the -sw 0 IP address for management GUI and telnet access. Unless you are carrying out activities to a specific CP, this prevents unpredictable results.

The switch name of the director can be up to 15 characters long, can include alpha, numeric, and underscore characters, and must begin with an alpha character. The default name for the director is “IBM_2109_M48”. Setting meaningful names for your switches simplifies the management of your SAN. Ideally, you should define an appropriate naming convention and use this to provide standardized names for your switches.

To customize the name, follow these steps:

1. Enter the **`switchName`** command with the new name in quotes.

   ```
   swDir:admin> switchName "IBM_2109_M48"
   Committing configuration...
   Done.
   IBM_2109_M48:admin>
   ```
2. Record the new name for future reference.

Each switch in the fabric must have a unique Domain ID. The Domain ID can be set using the **`configure`** command. You can also allow the Domain ID to be automatically set. The default Domain ID for the director is “1”.

To set the Domain ID, follow these steps:

1. Enter the **`fabricshow`** command to determine the current Domain IDs available.
2. Enter the **`switchdisable`** command to disable the director.
3. Enter the **`configure`** command.
4. Enter y at the Fabric parameters. prompt:

   ```
   Fabric parameters (yes, y, no, n): [no] y
   ```

5. Enter a unique Domain ID:

   ```
   Domain: (1..239) [1] 3
   ```

6. Complete the remaining prompts or press Ctrl+D to accept the other settings and to exit.
7. Enter the **`switchEnable`** command to re-enable the director.
8. Add SFPs and fiber optic cables to the ports as required.

   Note: The ports and cables used in trunking groups must meet specific requirements.

9. Remove the shipping plug from the ports to be used.
10. Position the SFP so that the key (the tab near the cable-end of the SFP) is on top, and insert the SFP into the port until it is firmly seated and the latching mechanism makes a clicking sound. For specific instructions, refer to the SFP manufacturer’s documentation.

    Note: The SFP module is keyed so that it can only be correctly inserted into the port. If the module does not slide in easily, try turning it over.

11. Connect the fiber optic cables to the SFPs as appropriate to the fabric topology by positioning each cable so that the key (the ridge on one side of the cable connector) is aligned with the slot in the SFP, then inserting the cable into the SFP until it is firmly seated and the latching mechanism makes a clicking sound.

    Note: The cable is keyed so that it can only be correctly inserted into the SFP. If the cable does not slide in easily, try turning it over.

12. Verify the correct operation of the switch.

13. Enter the following command at the Telnet prompt:

```
switchShow
```

> **Note:** This command provides information about the status of the switch and the ports. We strongly recommend backing up the configuration after any initial configuration changes, and periodically thereafter. This ensures that a complete configuration is available if ever required for uploading to a replacement switch. Issue a **`configUpload`** to the ftp server.

Setting Core PID format

The Core PID format parameter is a fabric wide parameter that has to be set in legacy 1-2 Gbps and 16 port switches (3534-S08, 2109-S16, 2109-F08 and 2109-F16) for port addressing capability with newer switches (2109-F32, 2005-H08, 2005-H16, 2109-M12, 2109-M14, 2109-M48, 2005-B16, 2005-B32 and 2005-B64).

Changing this parameter is disruptive to switch and fabric operation, as such we recommend setting this during fabric installation in order to minimize the impact when adding an H08, H16, F32, M12, M14, M48, B16, B32 or B64 at a later date.

> **Important:** The Core PID format must be set on *all* switches with FOS 2.X or 3.X if your SAN includes or will include a 2005-H08/H16, 2109-F32, 2109-M12, 2109-M14 or 2109-M48. By setting it without an F32, M12, M14, M48, B16, B32, B64 present, we are preparing our fabric for a future capacity upgrade with minimal disruption.

Before attempting to set the Core PID format, check to see if it is already set. Later switch models are shipped with the Core PID format already set to 1. Switches shipped with 4.x onwards FOS already have a Core PID format of 1.

To check and set the Core PID format, open a telnet session to the switch.

In Example 1-7 we issue the **`configShow “fabric”`** command:

Example 1-7 Checking the current PID using configshow

```
itsosw4:admin> configshow "fabric"
fabric.domain:  4
fabric.ops.BBCredit:    16
fabric.ops.E_D_TOV:     2000
fabric.ops.R_A_TOV:     10000
fabric.ops.dataFieldSize:       2112
fabric.ops.max_hops:    7
fabric.ops.mode.SeqSwitching:   0
fabric.ops.mode.fcpProbeDisable:        0
fabric.ops.mode.isolate:        0
fabric.ops.mode.longDistance:   0
fabric.ops.mode.noClassF:       0
fabric.ops.mode.pidFormat:      0
fabric.ops.mode.sync:   0
...
lines deleted for clarity
...

Type <CR> to continue, Q<CR> to stop:
```

Note: The new FOS version shows “Switch PID format” instead of Core PID. There are also three options (0, 1 or 2) at 4.4.x FOS and onwards.

Changing Core PID format might require a reboot of UNIX servers that bind by port ID.

Notice that the Core PID is set to zero, so we now set the Core PID by following these steps:

1. Disable the switch with the **`switchDisable`** command:

   ```
   switchDisable
   ```

2. Run the **`configure`** command:

   ```
   configure
   ```

3. The command prompts you to set Fabric Parameters. Type **`y`**:

   ```
   Fabric parameters (yes, y, no, n): [no] y
   ```

4. Press Enter to use default parameters for settings until you are prompted for the Core PID format setting. Set the parameter to **`1`**.

   ```
   Core Switch PID Format: (0..1) [0] 1
   ```

5. Continue to press Enter to skip other settings. You should get the following message:

   ```
   Committing configuration...done.
   ```

6. Enable the switch:

   ```
   switchenable
   ```

7. Fastboot the switch:

   ```
   fastboot
   ```

Setting the date

Now is also a good opportunity to set the date and time in the switch. Although a switch with the incorrect date and time will function properly, it is best to make them realistic, because they are used for time stamping during logging of events. We suggest setting these parameters prior to any further operations, because you will find this very helpful if you should have to troubleshoot at a later date.

We do this by using the **`date “MMDDhhmmYY”`** command, where MM = Month, DD = Day, hh = hour, mm = minutes, YY = Year, see Example 1-8.

Example 1-8 Setting the date and time

```
IBM_2005_B32:admin> date
Tue Nov  8 22:08:41 UTC 2006
IBM_2005_B32:admin>
IBM_2005_B32:admin>
IBM_2005_B32:admin> date "1908141706"
Tue Nov  8 14:17:00 UTC 2006
```

We have now completed the steps for our install, although we recommend upgrading to the latest level of firmware available at this time before making the switch available for use.

Refer to 1.9.7, “Upgrading the switch” on page 254 to perform this step.

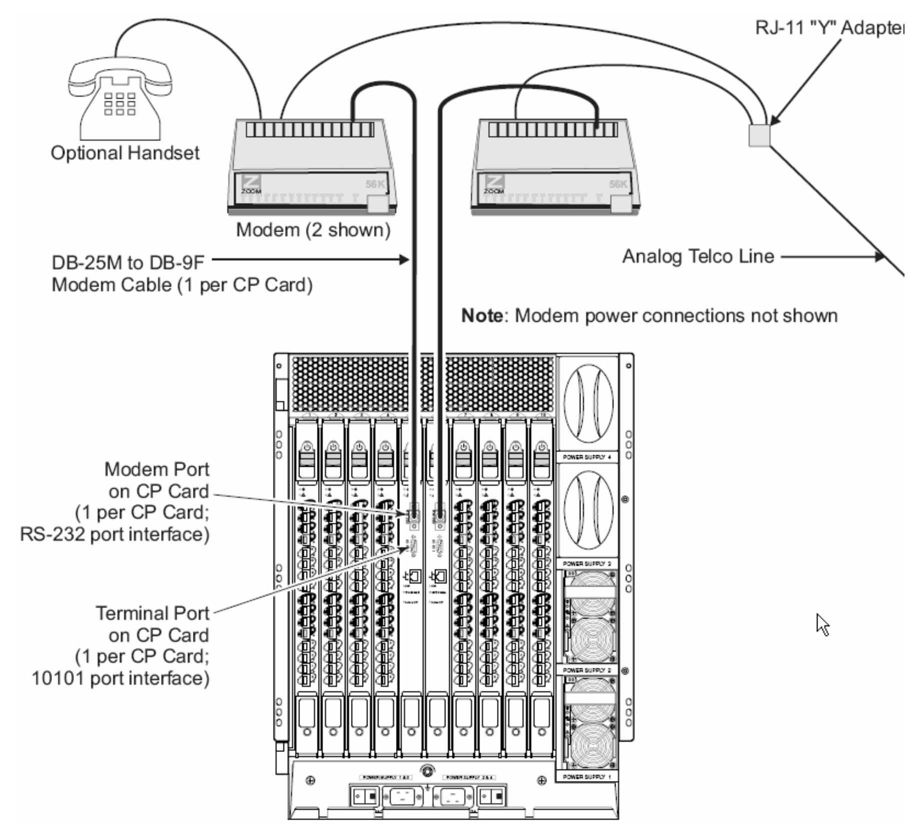
Optional modem setup

Each CP blade in the SAN256B contains a modem serial port for connection to a Hayes-compatible modem. The modem serial ports are wired as standard DTE ports and have the same commands, log in capabilities, and operational behavior as the terminal serial ports. However, asynchronous informational messages and other unsolicited text are not sent to the modem ports. No additional software is required to use modems with the director.

Note: The director detects modems only during power-on, reboot, or a CP blade failover sequence. Setting up the modems before powering on the director is recommended. For increased security, any active modem sessions are automatically disconnected if the modem cable is disconnected. For optimal security, disconnect the modem cable when it is not in use.

High availability of the modem connection can be ensured by connecting a separate modem to each CP blade and then connecting both modems to a shared telephone line. This ensures an available telephone connection to the active CP blade even if a failover occurs; however, it is necessary to log back in after a failover. When both CP blades are connected to a shared telephone line, callers are automatically dialed in to the active CP blade, which answers on the first ring. If the active CP blade cannot answer for any reason, the standby CP blade answers on the seventh ring and allows login to proceed.

Note: If a modem connection is set up, connect a modem to each CP blade, as shown in Figure 1-15.



RJ-11 "Y" Adapte
Optional Handset
Modem (2 shown)
DB-25M to DB-9F
Modem Cable (1 per CP Card)
Analog Telco Line
Note: Modem power connections not shown
Modem Port
on CP Card
(1 per CP Card;
RS-232 port interface)
Terminal Port
on CP Card
(1 per CP Card;
10101 port interface)

Figure 1-15 Optional modem line and data connections

Connecting modems

Note: Set up the modems before powering on the director and connect it to the fabric.

The following items are required to set up two modems to work with the director:

1. Two Hayes-compatible modems, such as the Zoom/Modem V.92 EXT Model 3049
2. Two standard modem cables, DB25 (male) to DB9 (female)
3. One RJ–11 “Y” adapter for standard Telco wiring or equivalent circuitry (three total connections)
4. One analog telephone line

Attention: Power off the director before connecting cables to the modem ports.

Complete the following steps to connect the modems to the director:

1. Optionally power off the director.
2. Set up the two modem units and corresponding power connections, but do not power on the modems until all cables are attached.
3. Connect the modem cables to the modems and to the director RS–232 modem ports.
4. Connect the telephone line inputs on the modems to the RJ–11 Y connector. This effectively places both modems on a single telephone line.
5. Optionally connect a telephone handset to one of the phone connections on the modems.
6. Connect the “Y” adapter to an appropriate analog telephone line and document the dial-in number for later use.
7. Power on the modems and verify that the Modem Ready indicator illuminates on both units.
8. Power on the director, or restart it if it was not powered off. This allows the director to recognize the modems.

When the modems are connected, you can use a Telco system to dial in to the modems and verify that they answer and communicate as expected. If a dial-out modem facility is not available, you can use a terminal emulation program on a computer workstation (or laptop) that has an attached modem.

This procedure is only required if a dial-out modem facility is not already available for testing the director modem connections.

Perform the following steps to set up the optional remote modem:

1. Connect the remote modem to the workstation, as shown in Figure 1-16.

2. Disable any serial communication programs running on the workstation (such as a synchronization program for a PDA).

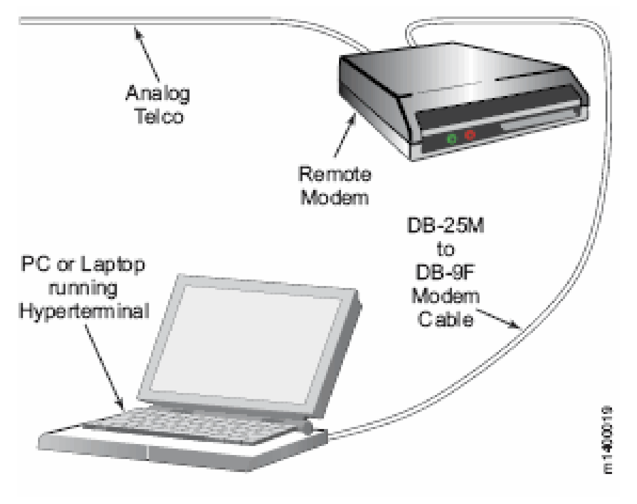

Analog
Telco
Remote
Modem
DB-25M
to
DB-9F
Modem
Cable
PC or Laptop
running
Hyperterminal
m1400019

Figure 1-16 Remote modem setup

3. Launch the terminal emulator application and configure as in Table 1-9.

Table 1-9 Configuration parameters.

Parameter	Value
Port Speed	115200*
Data protocol	Standard EC
Compression	Enabled
Flow Control	Hardware
Databits	8
Parity	None
Stop Bits	1
Modulation	Standard
*Port usually defaults to the highest speed supported by the modem, but might negotiate slower speed.	

4. Follow the instructions from the modem manufacturer to set up and verify modem operation.

Verifying the modem connection

This section provides information on how to verify that the modems are correctly connected.

> **Note:** This procedure requires either a Telco system to dial in to the modems or a terminal emulation program on a laptop or workstation that has an attached modem.

Complete the following steps to verify the modem connection:

1. Verify that both modem cables are firmly connected.
2. Power on the modems, if not already on.

   > **Note:** The modems must be powered on and operational before the director is powered on, to allow the director to detect the modems during boot.

3. Verify that both modems indicate that they are ready by illuminating their Clear to Send (CS), Terminal Ready (TR), and Modem Ready (MR) indicators. If this does not occur, ensure that the modems are connected to a power source and are powered on. Check all modem cable connections.
4. Verify that POST is complete on the director (a minimum of 3 minutes).
5. Dial in to the telephone number assigned to the director, using a Telco system to dial-in to the modems.
6. Observe the modem lamps: the Ring indicator should flash briefly as the telephone rings. If the Ring indicator does not flash on both units, recheck the incoming telephone lines to the modems.
7. Verify that after one ring, the modem associated with the active CP blade (usually in slot 5), illuminates the Off Hook (OH) indicator on the modem and a login prompt is presented to the remote client.
8. Log in to the switch from the remote client as admin. The default password is *password*.

   > **Note:** If the Off Hook indicator illuminates on the standby CP blade modem, recheck the modem cable connection to the active CP blade.

9. Log out of the modem session.

10. Remove the Telco connector from the active CP blade modem, leaving the Telco line from the standby CP blade connected to the "Y" connector. See Figure 1-15 on page 57.

    > **Note:** The modem session is automatically disconnected if the modem cable is detached while a session is active.

11. Dial in to the telephone number assigned to the director.
12. Observe the modem lamps. The Ring indicator should flash only on the modem connected to the standby CP blade.
13. Verify that after seven rings, the Off Hook indicator on the standby CP blade modem is illuminated. A login prompt is presented to the remote client, and a message confirms that the standby CP blade is being logged in to. You can log in or disconnect the session, as desired.
14. Reconnect the Telco connector to the active CP blade modem. The director modems are ready for use.

1.7.4 SAN16B Quick Setup with EZSwitchSetup v2.1.0

This starter kit greatly simplifies the setup and implementation of a SAN16B switch. The kit ships with the switch and contains a serial cable and a CD containing the setup software. It makes the switch setup as simple as a "click-and-go" solution.

If we follow the standard switch configuration practice, we implement a new switch by connecting a serial cable, setting up a tool such as Hyperterm to communicate, and implementing the **`ipaddrset`** command to configure the IP address. From this point we can then connect to the network via an ethernet cable, using a Web browser to access WebTools or alternatively using telnet to enter CLI mode and configure the switch further. From here we are able to set up zoning, assuming all devices are connected and also switch status monitoring using WebTools, SNMP or an external application.

Now, EZSwitchSetup greatly simplifies this by automatically walking you through all the steps above using its own GUI-based interface.

In the following pages, we walk through using EZSwitchSetup to configure a SAN-16B switch.

Setup

Before starting, you have to obtain an IP address, subnet mask, and default gateway address for the switch. Using either a Windows machine close to the switch, or a laptop, insert the CD, which will start automatically, as shown in Figure 1-17. Click **OK** to start this installation.

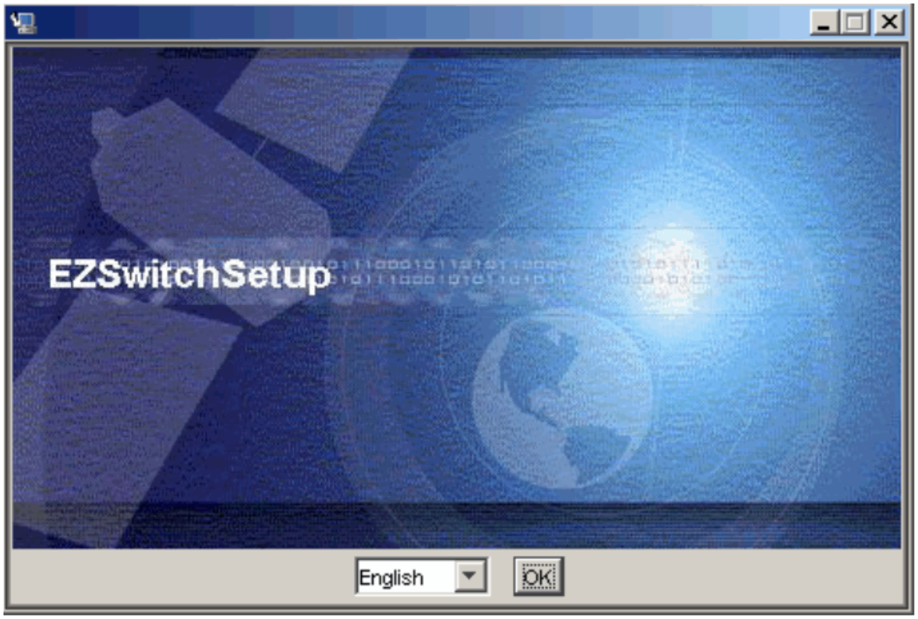
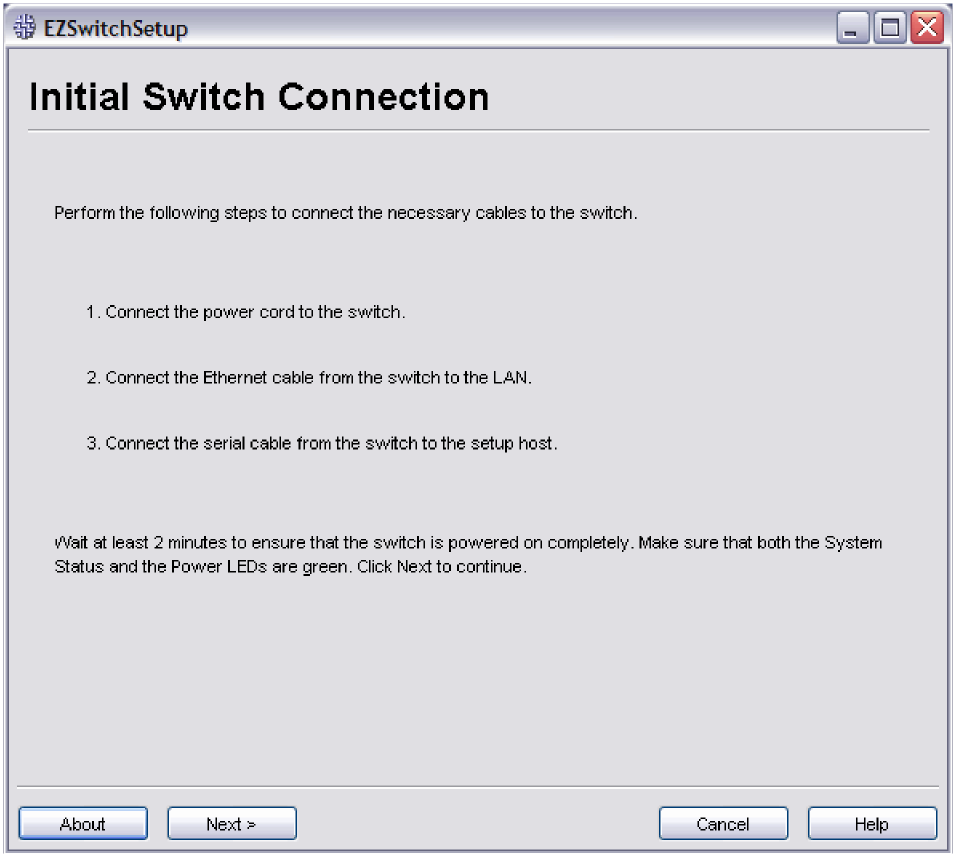


Figure 1-17 EZSwitchSetup startup panel

InstallAnywhere guides you through the simple five-step installation. The EZSwitchSetup program runs automatically once the installation is complete.

Following the on-screen instructions seen in Figure 1-18, connect the power cord to the switch, the Ethernet cable between the laptop and switch, and connect the serial cable from your laptop to the switch. Wait for the switch to fully power on before progressing. It might take up to 3 minutes for the switch to be in a ready state with both the System Status and Power LEDs green.



Initial Switch Connection

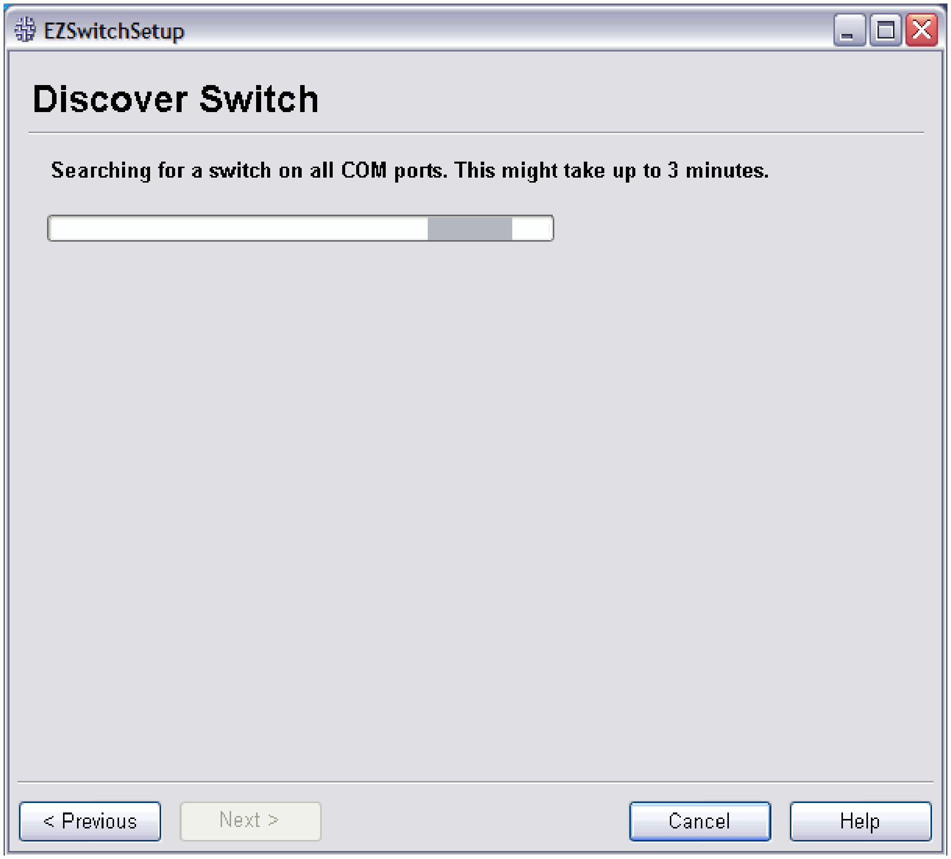
Perform the following steps to connect the necessary cables to the switch.

1. Connect the power cord to the switch.
2. Connect the Ethernet cable from the switch to the LAN.
3. Connect the serial cable from the switch to the setup host.

Wait at least 2 minutes to ensure that the switch is powered on completely. Make sure that both the System Status and the Power LEDs are green. Click Next to continue.

Figure 1-18 EZSwitchSetup initial panel

When you click **Next**, the software starts a discovery by checking all the COM ports as seen in Figure 1-19. When the switch is found, you can move to the next panel.

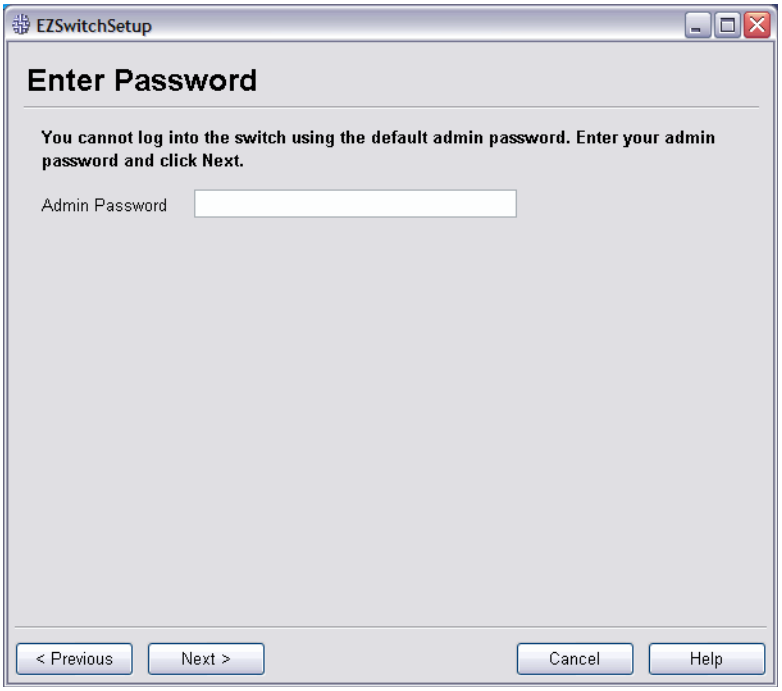

EZSwitchSetup
Discover Switch

Searching for a switch on all COM ports. This might take up to 3 minutes.

< Previous
Next >
Cancel
Help

Figure 1-19 EZSwitchSetup discovering the switch

EZSwitchSetup logs into the switch using the admin id. If, for whatever reason, the default password has changed, EZSwitchSetup prompts you for the new password. This is shown in Figure 1-20.



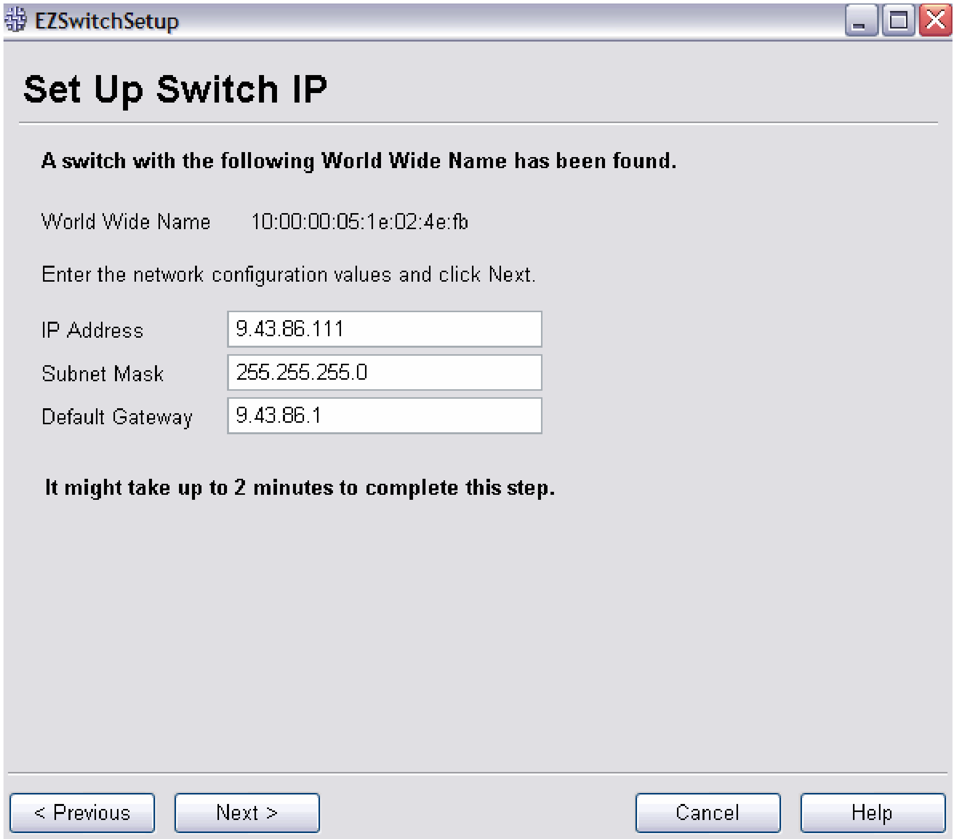
Enter Password

You cannot log into the switch using the default admin password. Enter your admin password and click Next.

Admin Password

Figure 1-20 EZSwitchSetup prompting for the new password

At the next panel, Figure 1-21, replace the default IP settings with your own configuration. Enter values for the IP address, Subnet Mask and default gateway and click **Next**.



Set Up Switch IP

A switch with the following World Wide Name has been found.

World Wide Name 10:00:00:05:1e:02:4e:fb

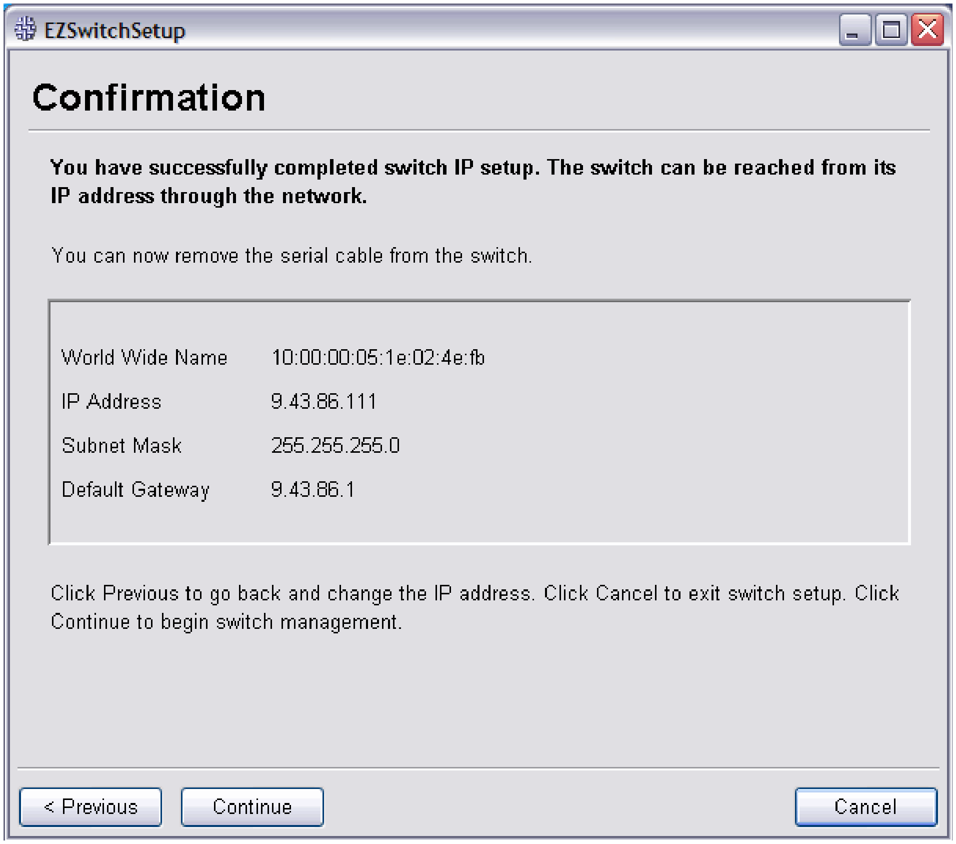
Enter the network configuration values and click Next.

IP Address 9.43.86.111
Subnet Mask 255.255.255.0
Default Gateway 9.43.86.1

It might take up to 2 minutes to complete this step.

Figure 1-21 Setting up IP, Subnet, and Gateway

Now the switch IP settings are complete, see Figure 1-22. We click **Continue** and this spawns the WebToolsEZ session. This is just an applet plug-in for your existing browser, so if you do not have a browser plug-in installed, then this part fails. If you have a firewall enabled, you might have to permit access to the Internet in order to continue.



Confirmation

You have successfully completed switch IP setup. The switch can be reached from its IP address through the network.

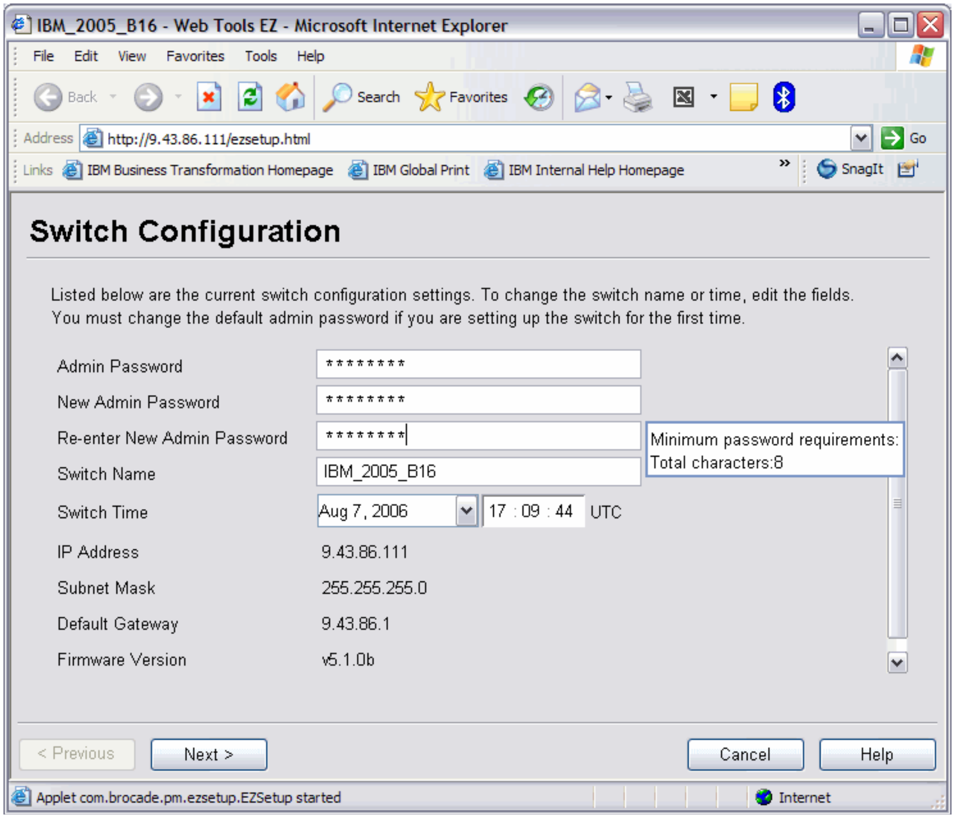
You can now remove the serial cable from the switch.

World Wide Name	10:00:00:05:1e:02:4e:fb
IP Address	9.43.86.111
Subnet Mask	255.255.255.0
Default Gateway	9.43.86.1

Click Previous to go back and change the IP address. Click Cancel to exit switch setup. Click Continue to begin switch management.

Figure 1-22 IP address setup complete

As this is a new switch out of the box, we see the Switch Setup wizard. However, if this were not a new switch, then WebTools would present the switch manager as seen in Figure 1-23.


IBM_2005_B16 - Web Tools EZ - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
Go
Links
IBM Business Transformation Homepage
IBM Global Print
IBM Internal Help Homepage
SnagIt
< Previous
Next >
Cancel
Help
Internet

http://9.43.86.111/ezsetup.html

Switch Configuration

Listed below are the current switch configuration settings. To change the switch name or time, edit the fields. You must change the default admin password if you are setting up the switch for the first time.

Admin Password: ********
New Admin Password: ********
Re-enter New Admin Password: ********
Minimum password requirements: Total characters:8
Switch Name: IBM_2005_B16
Switch Time: Aug 7, 2006 17 : 09 : 44 UTC
IP Address: 9.43.86.111
Subnet Mask: 255.255.255.0
Default Gateway: 9.43.86.1
Firmware Version: v5.1.0b

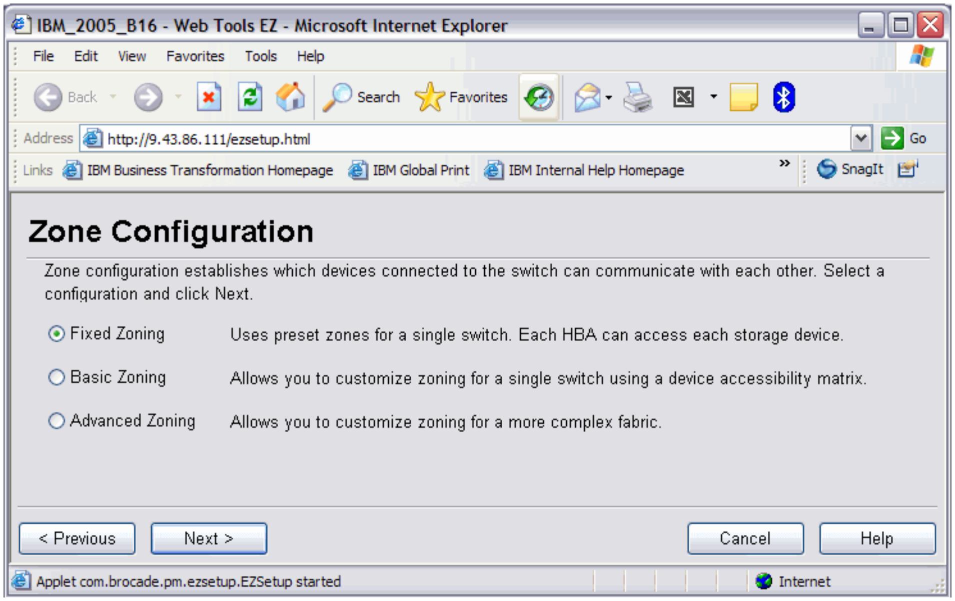
Applet com.brocade.pm.ezsetup.EZSetup started

Figure 1-23 Switch Setup Wizard

We now set up the admin password, switch name, and switch time.

EZsetup can be re accessed at a later date/time by entering ***switchIP*/EZsetup.html** as the Address field in a Web browser, or alternatively by selecting the setup option from the Switch manager.

When we have set up these values, clicking **Next** brings us to the zoning configuration panel, Figure 1-24.


IBM_2005_B16 - Web Tools EZ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
IBM Business Transformation Homepage
IBM Global Print
IBM Internal Help Homepage
SnagIt
< Previous
Next >
Cancel
Help
Internet

http://9.43.86.111/ezsetup.html

Zone Configuration

Zone configuration establishes which devices connected to the switch can communicate with each other. Select a configuration and click Next.

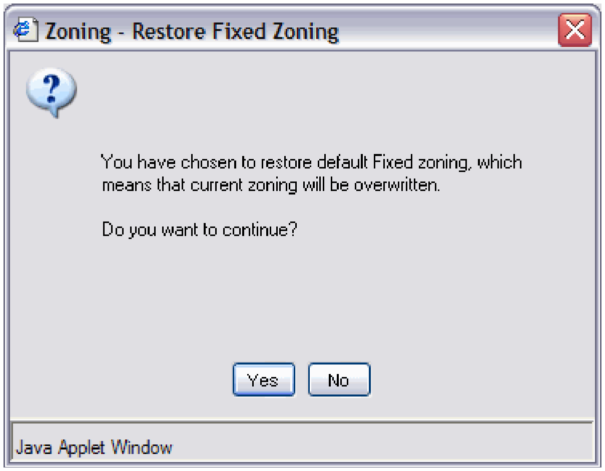
● Fixed Zoning	Uses preset zones for a single switch. Each HBA can access each storage device.
○ Basic Zoning	Allows you to customize zoning for a single switch using a device accessibility matrix.
○ Advanced Zoning	Allows you to customize zoning for a more complex fabric.

Applet com.brocade.pm.ezsetup.EZSetup started

Figure 1-24 Zoning setup panel

Here we are presented with three options: Fixed Zoning, with one HBA port mapped to One Storage port; Basic Zoning, which allows customized zoning based upon a matrix where HBAs and Storage should be pre-connected; and Advanced zoning, as it is today.

After selecting Fixed Zoning, you are asked whether you want to restore the default, Fixed zoning, and consequently overwrite any current zoning that is in place. This is shown in Figure 1-25.


Zoning - Restore Fixed Zoning

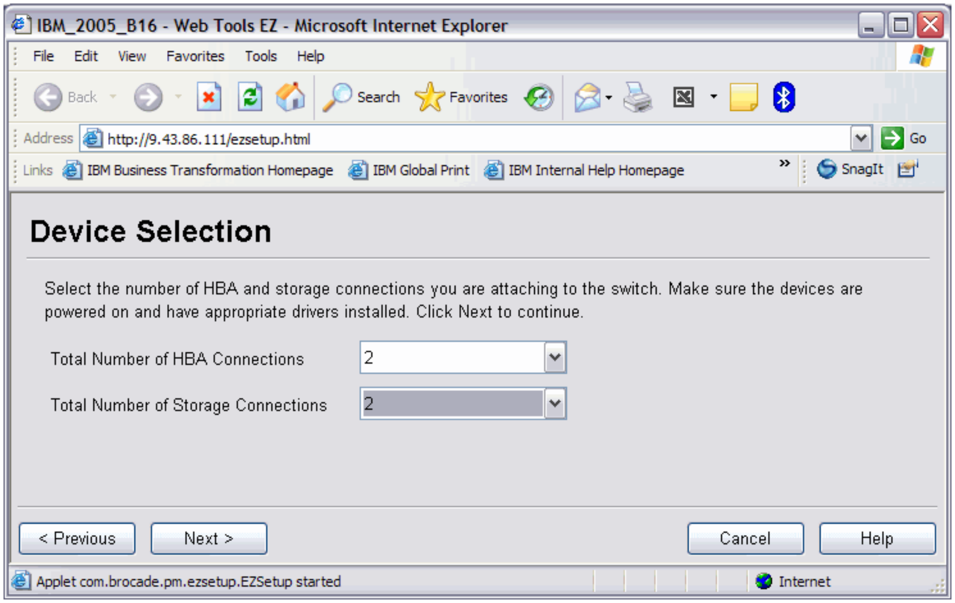
You have chosen to restore default Fixed zoning, which means that current zoning will be overwritten.

Do you want to continue?

Yes
No
Java Applet Window

Figure 1-25 Restore Fixed Zoning

In the following panel, Figure 1-26, we have the device selection panel. Here we select the number of host HBA ports and Storage Connectors that we will connect to the switch.


IBM_2005_B16 - Web Tools EZ - Microsoft Internet Explorer

File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
IBM Business Transformation Homepage
IBM Global Print
IBM Internal Help Homepage
SnagIt

http://9.43.86.111/ezsetup.html

Device Selection

Select the number of HBA and storage connections you are attaching to the switch. Make sure the devices are powered on and have appropriate drivers installed. Click Next to continue.

Total Number of HBA Connections 2

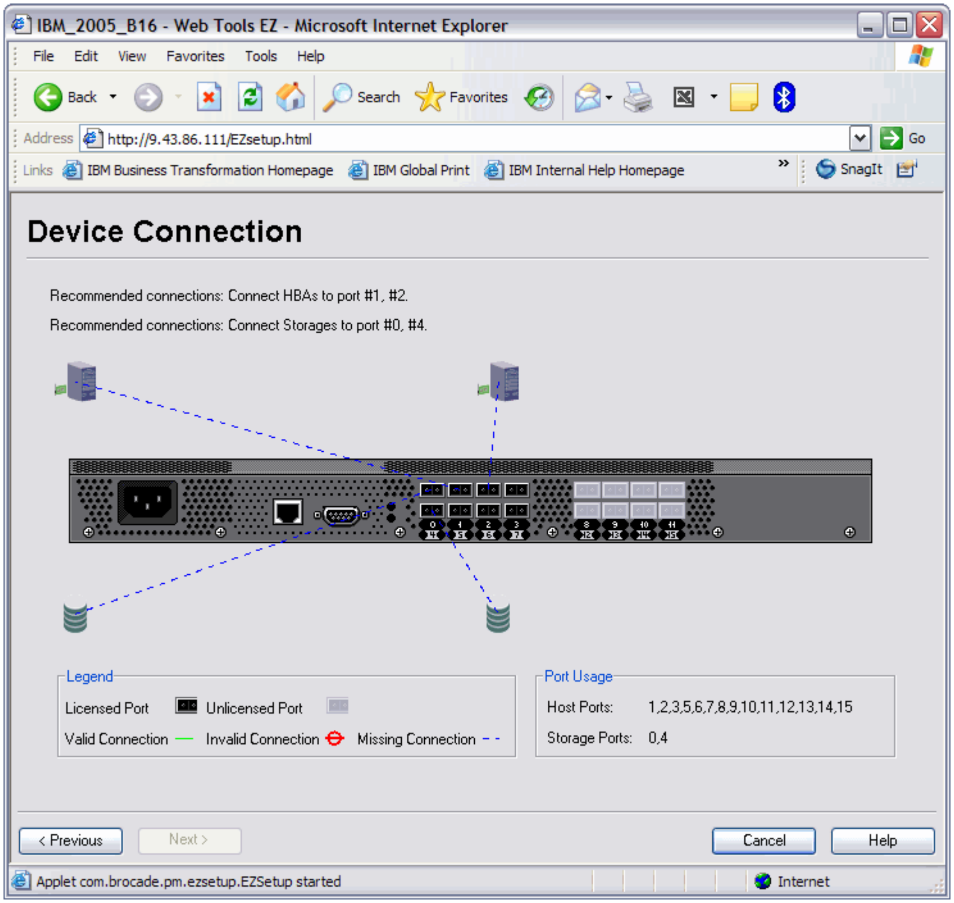
Total Number of Storage Connections 2

< Previous
Next >
Cancel
Help
Internet

Applet com.brocade.pm.ezsetup.EZSetup started

Figure 1-26 Selecting the number of host and storage devices

EZSwitch then displays the device connection window, Figure 1-27, which suggests the ports that should be used for the requested connections. The next step is to physically connect the hosts and storage as suggested by the software.


IBM_2005_B16 - Web Tools EZ - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Go
Links
IBM Business Transformation Homepage
IBM Global Print
IBM Internal Help Homepage
SnagIt
0
1
2
3
8
9
10
11
< Previous
Next >
Cancel
Help
Internet

Address http://9.43.86.111/EZsetup.html

Device Connection

Recommended connections: Connect HBAs to port #1, #2.

Recommended connections: Connect Storages to port #0, #4.

Legend

Licensed Port ▪ Unlicensed Port ▫

Valid Connection — Invalid Connection ⊖ Missing Connection - -

Port Usage

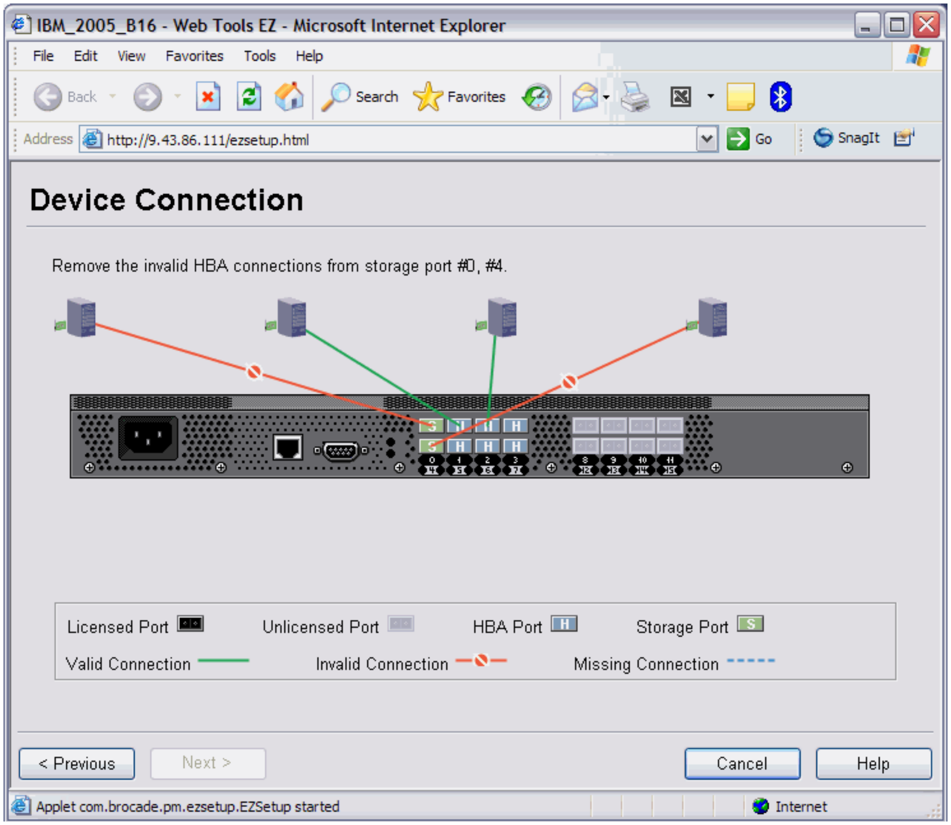
Host Ports: 1,2,3,5,6,7,8,9,10,11,12,13,14,15

Storage Ports: 0,4

Applet com.brocade.pm.ezsetup.EZSetup started

Figure 1-27 Device connection status panel for fixed zoning

Figure 1-28 shows how we have connected our devices. A valid connection is shown with a green line, an invalid connection is shown with a red line containing a stop circle, and a missing connection is shown with a dashed blue line.

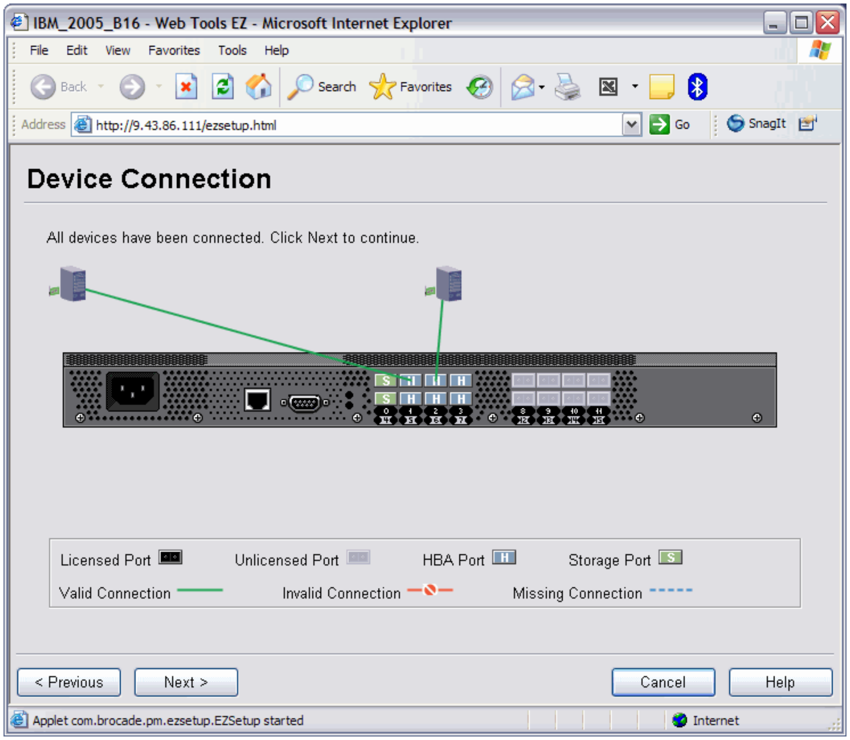

IBM_2005_B16 - Web Tools EZ - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://9.43.86.111/ezsetup.html
Go
SnagIt
Licensed Port
Unlicensed Port
HBA Port
Storage Port
Valid Connection
Invalid Connection
Missing Connection
< Previous
Next >
Cancel
Help
Applet com.brocade.pm.ezsetup.EZSetup started
Internet

Device Connection

Remove the invalid HBA connections from storage port #0, #4.

Figure 1-28 Devices connected in EZ Switch Setup Wizard

In our example, you might notice that the storage components connected to ports 0 and 4 are displayed as **Invalid Connection**. This is caused because the storage device used has been configured to be both an Initiator and Target. The EZSwitch wizard cannot manage this situation, as generally this would occur in a more advanced configuration where you would not use the EZSwitch Wizard. However you can circumvent this problem by removing the storage from the configuration and then add this after the initial Switch Setup process is complete. See Figure 1-29 for details.



IBM_2005_B16 - Web Tools EZ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://9.43.86.111/ezsetup.html
Go SnagIt

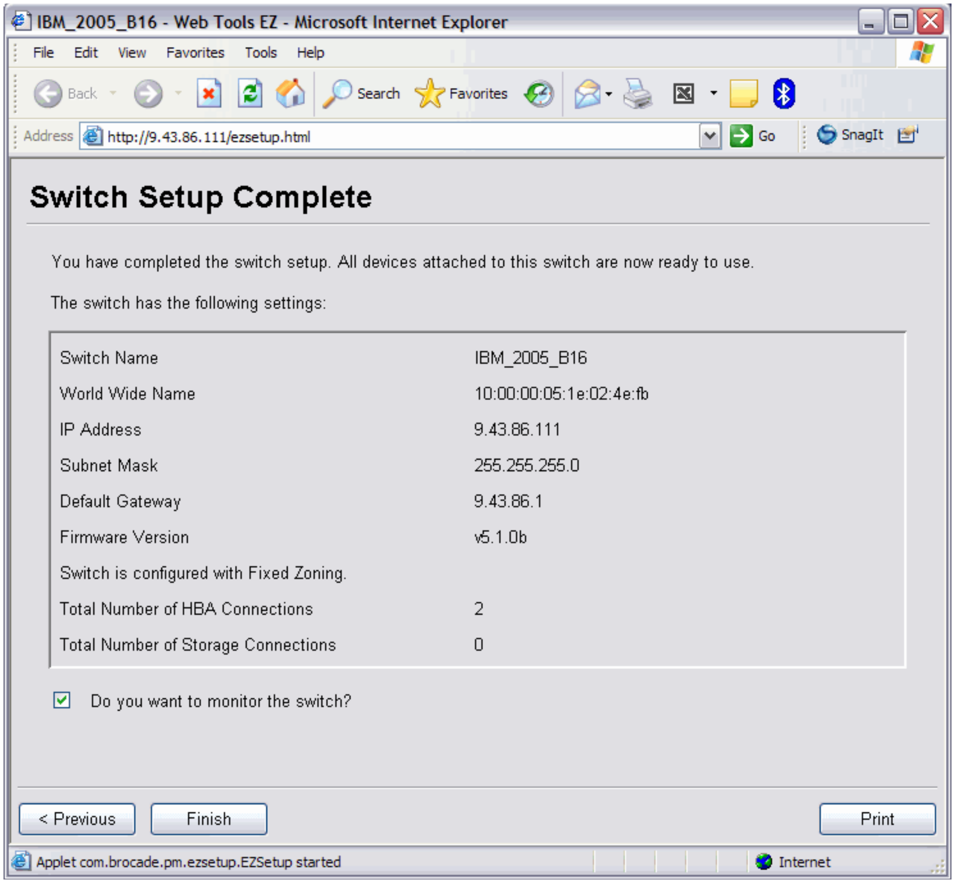
Device Connection

All devices have been connected. Click Next to continue.

S
H
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Licensed Port
Unlicensed Port
HBA Port
Storage Port
Valid Connection
Invalid Connection
Missing Connection
< Previous
Next >
Cancel
Help
Internet

Applet com.brocade.pm.ezsetup.EZSetup started

Figure 1-29 Adding two hosts with EZ Switch Setup Wizard


IBM_2005_B16 - Web Tools EZ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://9.43.86.111/ezsetup.html Go SnagIt

Switch Setup Complete

You have completed the switch setup. All devices attached to this switch are now ready to use.

The switch has the following settings:

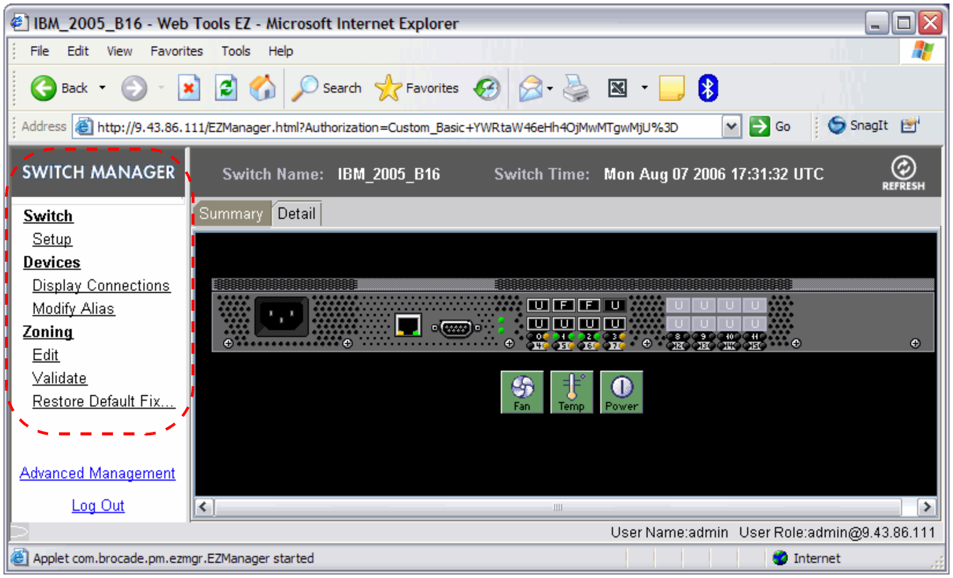
Switch Name	IBM_2005_B16
World Wide Name	10:00:00:05:1e:02:4e:fb
IP Address	9.43.86.111
Subnet Mask	255.255.255.0
Default Gateway	9.43.86.1
Firmware Version	v5.1.0b
Switch is configured with Fixed Zoning.	
Total Number of HBA Connections	2
Total Number of Storage Connections	0

☑ Do you want to monitor the switch?

< Previous
Finish
Print
Applet com.brocade.pm.ezsetup.EZSetup started
Internet

Figure 1-30 Final panel from the setup process

The final setup panel (Figure 1-31) shows a summary of the switch and lets us check a checkbox to spawn the switch manager.


IBM_2005_B16 - Web Tools EZ - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
Go
SnagIt
SWITCH MANAGER
REFRESH
Summary
Detail
Switch
Setup
Devices
Display Connections
Modify Alias
Zoning
Edit
Validate
Restore Default Fix...
Advanced Management
Log Out
Fan
Temp
Power
Internet

Address: http://9.43.86.111/EZManager.html?Authorization=Custom_Basic+YWRtaW46eHh4OjMwMTgwMjU%3D

Switch Name: IBM_2005_B16

Switch Time: Mon Aug 07 2006 17:31:32 UTC

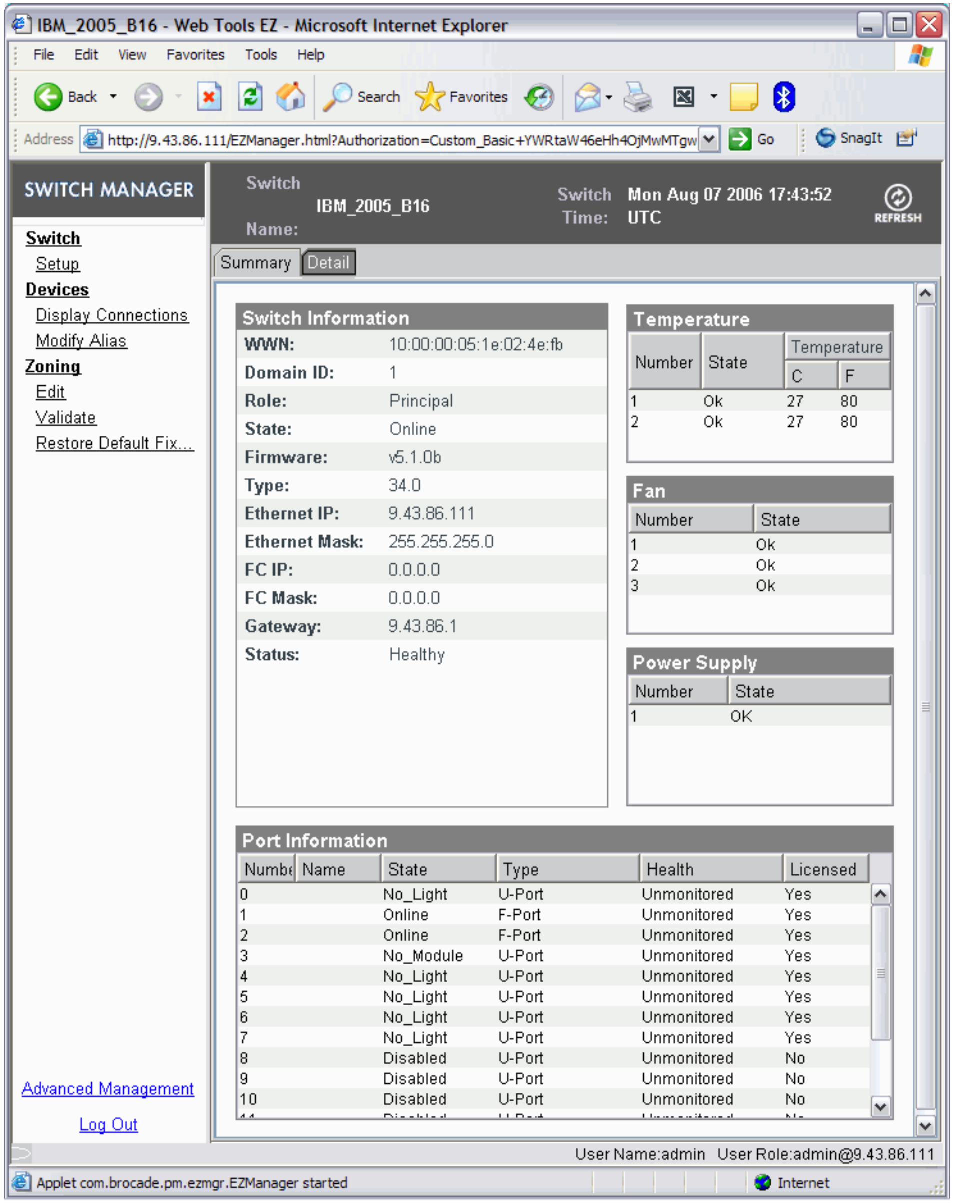
User Name:admin User Role:admin@9.43.86.111

Applet com.brocade.pm.ezmgr.EZManager started

Figure 1-31 Switch manager summary panel

After selecting the Switch Manager Launch option and logging into the switch, we are presented with the Switch Manager Summary panel as seen in Figure 1-32. Here we can see the switch name, switch time, user names and roles, switch IP address and a switch summary.

The left hand column gives us access to view further switch information, devices connections and zoning configurations. At the bottom of that column we have access to launch advanced zoning options or logout.


IBM_2005_B16 - Web Tools EZ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://9.43.86.111/EZManager.html?Authorization=Custom_Basic+YWRtaW46eHh4OjMwMTgw
Go SnagIt
SWITCH MANAGER
Switch
Setup
Devices
Display Connections
Modify Alias
Zoning
Edit
Validate
Restore Default Fix...
Advanced Management
Log Out
REFRESH
Summary Detail

Switch Name: IBM_2005_B16

Switch Time: Mon Aug 07 2006 17:43:52 UTC

Switch Information

WWN:	10:00:00:05:1e:02:4e:fb
Domain ID:	1
Role:	Principal
State:	Online
Firmware:	v5.1.0b
Type:	34.0
Ethernet IP:	9.43.86.111
Ethernet Mask:	255.255.255.0
FC IP:	0.0.0.0
FC Mask:	0.0.0.0
Gateway:	9.43.86.1
Status:	Healthy

Temperature

Number	State	Temperature	
		C	F
1	Ok	27	80
2	Ok	27	80

Fan

Number	State
1	Ok
2	Ok
3	Ok

Power Supply

Number	State
1	OK

Port Information

Numbe	Name	State	Type	Health	Licensed
0		No_Light	U-Port	Unmonitored	Yes
1		Online	F-Port	Unmonitored	Yes
2		Online	F-Port	Unmonitored	Yes
3		No_Module	U-Port	Unmonitored	Yes
4		No_Light	U-Port	Unmonitored	Yes
5		No_Light	U-Port	Unmonitored	Yes
6		No_Light	U-Port	Unmonitored	Yes
7		No_Light	U-Port	Unmonitored	Yes
8		Disabled	U-Port	Unmonitored	No
9		Disabled	U-Port	Unmonitored	No
10		Disabled	U-Port	Unmonitored	No

User Name:admin User Role:admin@9.43.86.111

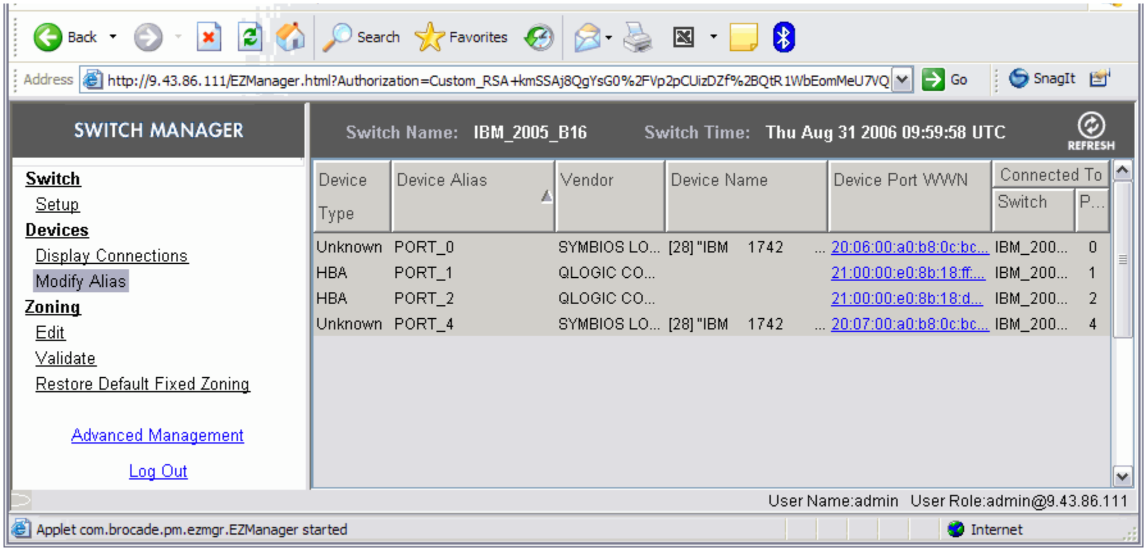
Applet com.brocade.pm.ezmgr.EZManager started

Figure 1-32 Switch Manager detailed view

The **Switch Detail** view shows further switch information, temperature, fans, power supplies, firmware, domain WWNs, and ports.

Selecting **Switch Setup** from the menu simply returns us to the initial setup panel, as seen in Figure 1-23 on page 68.

Selecting the **Device View** option, as shown in Figure 1-33, we are presented with a list of attached devices which are currently online. Clicking a WWN gives us further information about this device.


Back
Search
Favorites
Address
Go
SnagIt
SWITCH MANAGER
REFRESH
Switch
Setup
Devices
Display Connections
Modify Alias
Zoning
Edit
Validate
Restore Default Fixed Zoning
Advanced Management
Log Out
Internet

http://9.43.86.111/EZManager.html?Authorization=Custom_RSA+kmSSAj8QgYsG0%2FVp2pCUizDZf%2BQtR1WbEomMeU7VQ

Switch Name: IBM_2005_B16 Switch Time: Thu Aug 31 2006 09:59:58 UTC

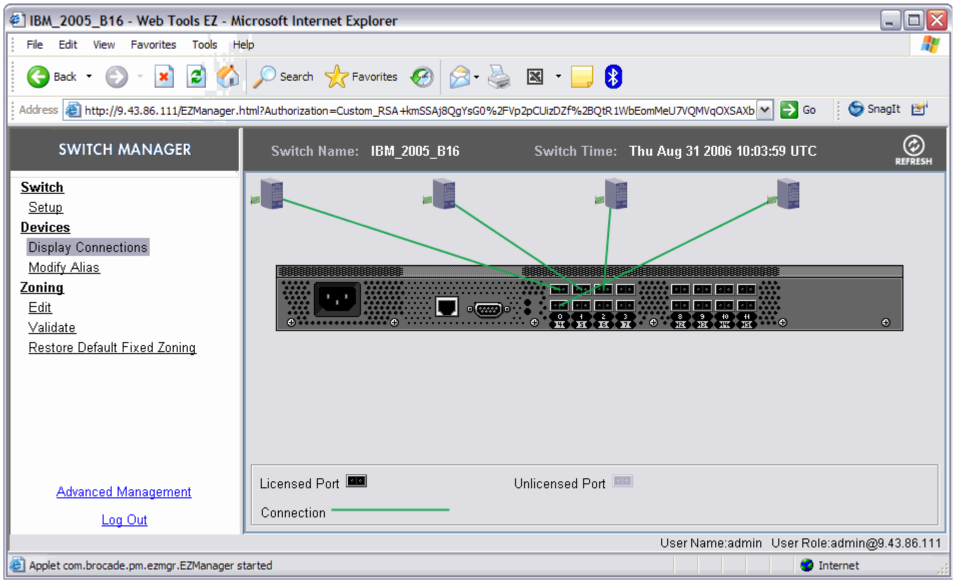
Device Type	Device Alias	Vendor	Device Name	Device Port WWN	Connected To	
					Switch	P...
Unknown	PORT_0	SYMBIOS LO...	[28] "IBM 1742 ...	20:06:00:a0:b8:0c:bc...	IBM_200...	0
HBA	PORT_1	QLOGIC CO...		21:00:00:e0:8b:18:ff:...	IBM_200...	1
HBA	PORT_2	QLOGIC CO...		21:00:00:e0:8b:18:d...	IBM_200...	2
Unknown	PORT_4	SYMBIOS LO...	[28] "IBM 1742 ...	20:07:00:a0:b8:0c:bc...	IBM_200...	4

User Name:admin User Role:admin@9.43.86.111

Applet com.brocade.pm.ezmgr.EZManager started

Figure 1-33 Device View

From the Devices option, we choose **Display Connections** and this presents a panel showing a graphical representation of Hosts and Storage connected to this switch. See Figure 1-34. If fixed zoning is in place, then these connections are validated.


IBM_2005_B16 - Web Tools EZ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
SnagIt
SWITCH MANAGER
Switch
Setup
Devices
Display Connections
Modify Alias
Zoning
Edit
Validate
Restore Default Fixed Zoning
Advanced Management
Log Out
REFRESH
Licensed Port
Unlicensed Port
Connection
Internet

http://9.43.86.111/EZManager.html?Authorization=Custom_RSA+kmSSAj8QgYsG0%2FVp2pCUizDZf%2BQtR1WbEomMeU7VQMVqOXSAXb

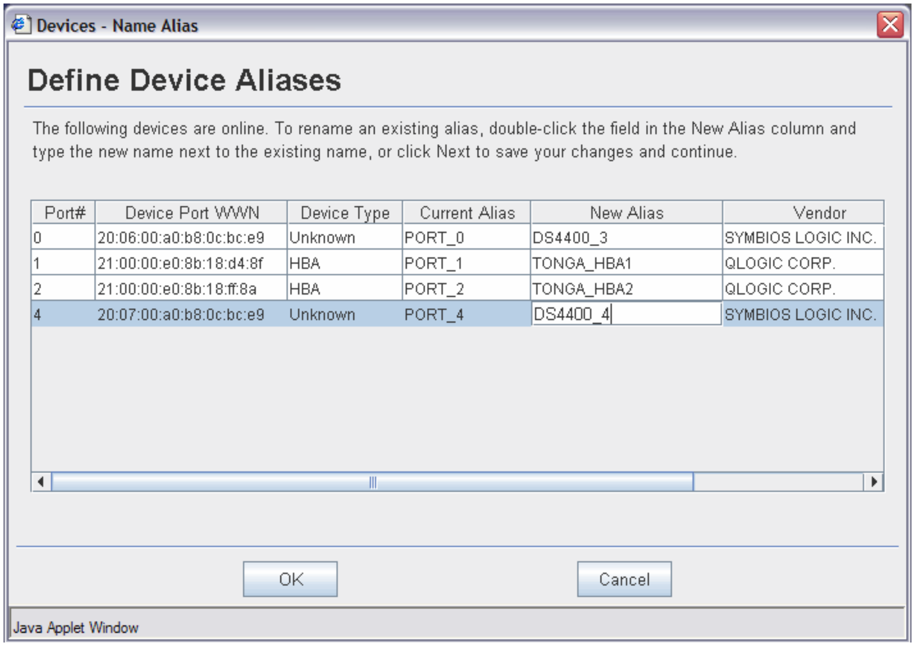
Switch Name: IBM_2005_B16 Switch Time: Thu Aug 31 2006 10:03:59 UTC

User Name:admin User Role:admin@9.43.86.111

Applet com.brocade.pm.ezmgr.EZManager started

Figure 1-34 Connection View

From Devices, we click **Modify Alias** to display the device alias wizard as shown in Figure 1-35.



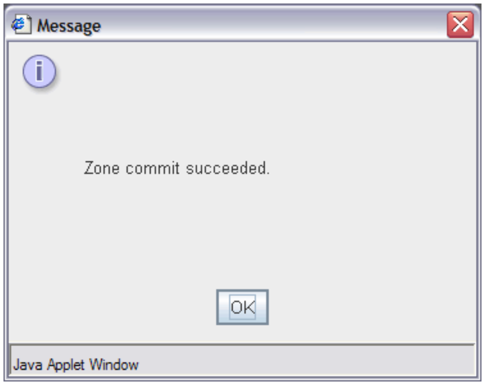
Define Device Aliases

The following devices are online. To rename an existing alias, double-click the field in the New Alias column and type the new name next to the existing name, or click Next to save your changes and continue.

Port#	Device Port WWN	Device Type	Current Alias	New Alias	Vendor
0	20:06:00:a0:b8:0c:bc:e9	Unknown	PORT_0	DS4400_3	SYMBIOS LOGIC INC.
1	21:00:00:e0:8b:18:d4:8f	HBA	PORT_1	TONGA_HBA1	QLOGIC CORP.
2	21:00:00:e0:8b:18:ff:8a	HBA	PORT_2	TONGA_HBA2	QLOGIC CORP.
4	20:07:00:a0:b8:0c:bc:e9	Unknown	PORT_4	DS4400_4	SYMBIOS LOGIC INC.

Figure 1-35 Device alias wizard

Following the on-screen instructions, we change the device aliases to something more meaningful. Clicking **OK** commits the alias details to the switch, and we are advised that the zone commit has succeeded; see Figure 1-36.



Zone commit succeeded.

Figure 1-36 Zone commit succeeded

Selecting Edit from the Zoning menu displays the current Device Connection view, as shown in Figure 1-37.

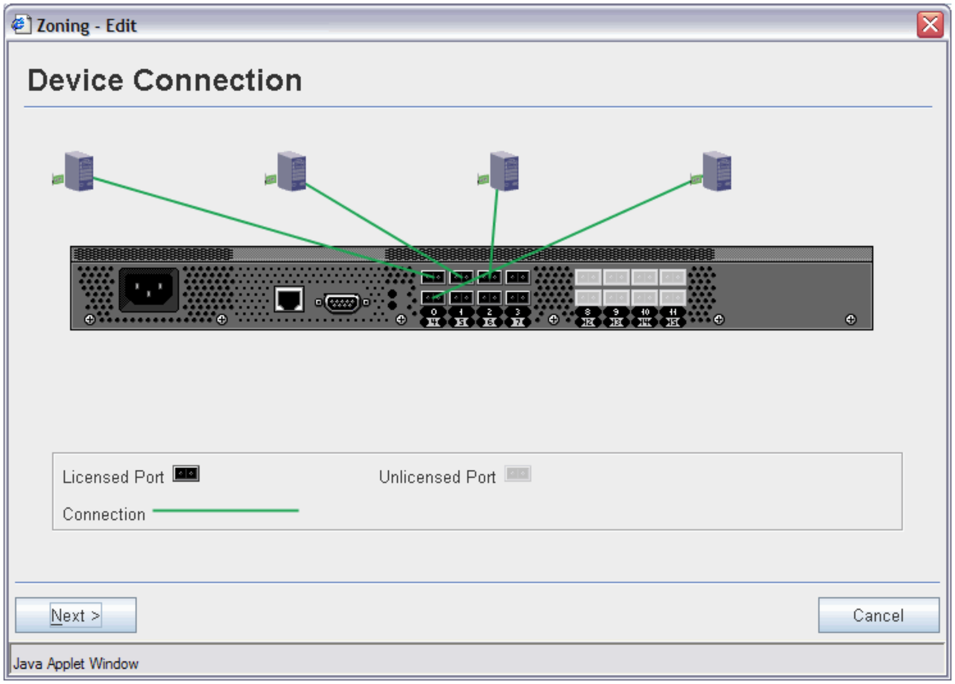
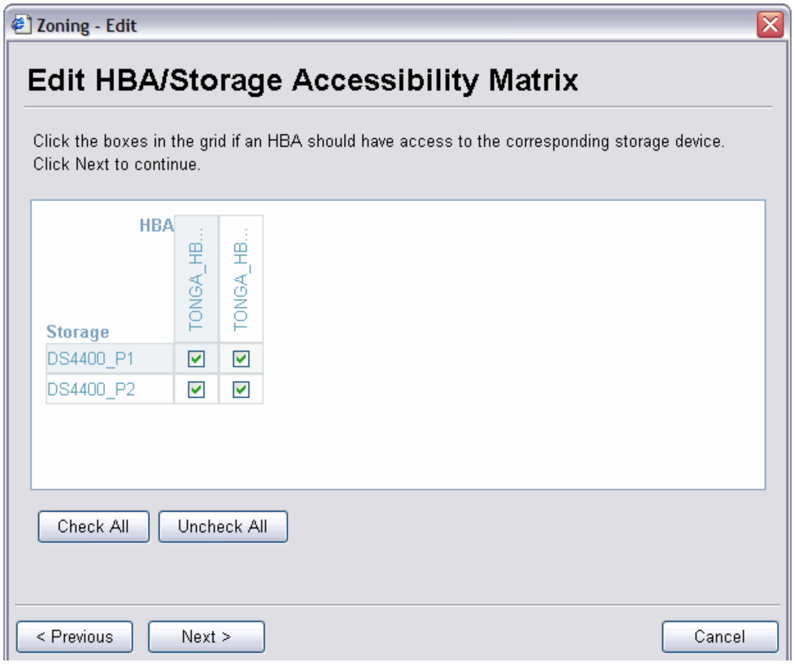

Zoning - Edit
Device Connection
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Licensed Port
Unlicensed Port
Connection
Next >
Cancel
Java Applet Window

Figure 1-37 Device Connection

In our example we used a disk configured with advanced functions (mirroring) and as such, our storage units in slots 0 and 4 are presented as hosts.

Clicking **Next** brings us to the Define Device Alias window. As we have already configured our aliases, we click **Next** to continue. We are then presented with the Edit HBA/Storage Accessibility Matrix as shown in Figure 1-38. From the matrix we check the HBA to Storage connections that we require and click **Next** to proceed.



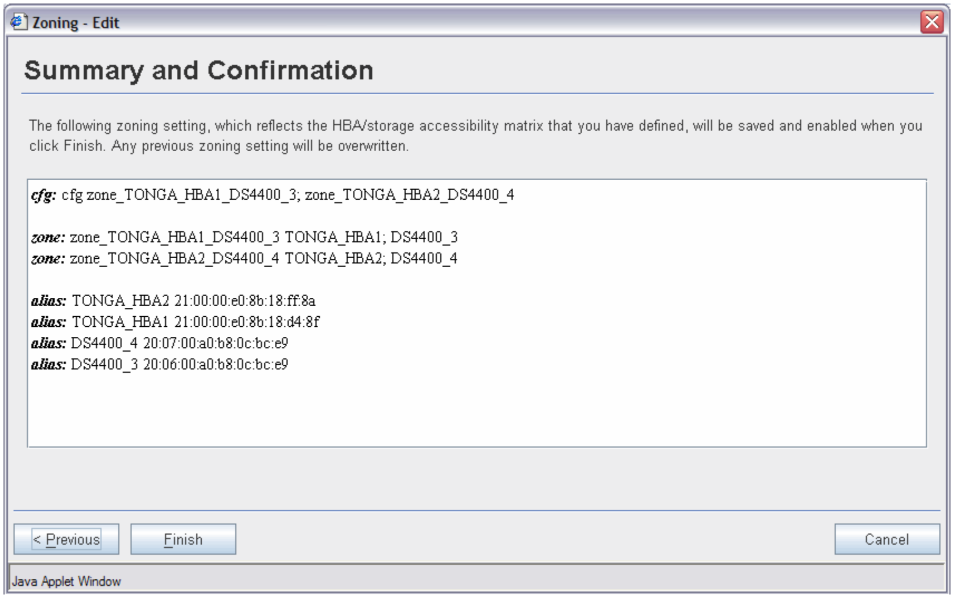
Edit HBA/Storage Accessibility Matrix

Click the boxes in the grid if an HBA should have access to the corresponding storage device.
Click Next to continue.

HBA Storage	TONGA_HB...	TONGA_HB...
DS4400_P1	☑	☑
DS4400_P2	☑	☑

Figure 1-38 HBA/Storage Accessibility Matrix

Figure 1-39 shows Summary and Confirmation information on the selected settings. On clicking **Finish**, the selected zoning settings are saved and enabled; this replaces any previous settings that were configured. A pop-up window is displayed to confirm that the Zone commit has succeeded.



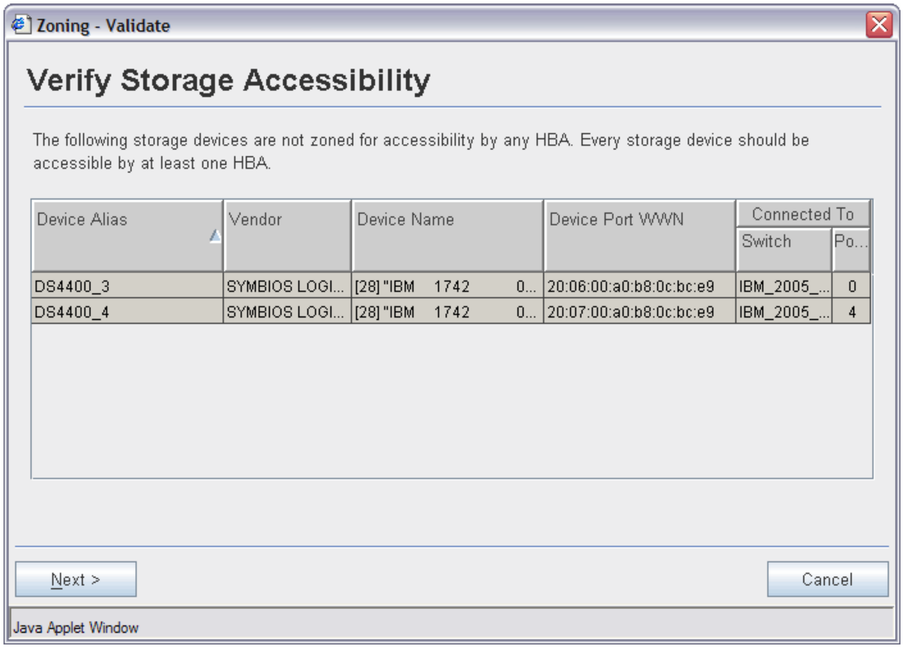
Summary and Confirmation

The following zoning setting, which reflects the HBA/storage accessibility matrix that you have defined, will be saved and enabled when you click Finish. Any previous zoning setting will be overwritten.

```
cfg: cfg zone_TONGA_HBA1_DS4400_3; zone_TONGA_HBA2_DS4400_4

zone: zone_TONGA_HBA1_DS4400_3 TONGA_HBA1; DS4400_3
zone: zone_TONGA_HBA2_DS4400_4 TONGA_HBA2; DS4400_4

alias: TONGA_HBA2 21:00:00:e0:8b:18:ff:8a
alias: TONGA_HBA1 21:00:00:e0:8b:18:d4:8f
alias: DS4400_4 20:07:00:a0:b8:0c:bc:e9
alias: DS4400_3 20:06:00:a0:b8:0c:bc:e9
```

Figure 1-39 Zoning-Edit Summary and Confirmation

We can also use the Validate selection from the Zoning menu to validate our configuration. Selecting Validate displays Figure 1-40. The zoning matrix is validated, checking that every storage device is accessible by at least one HBA and that every HBA should have at least one storage device. If we have inaccessible devices, these are reported.

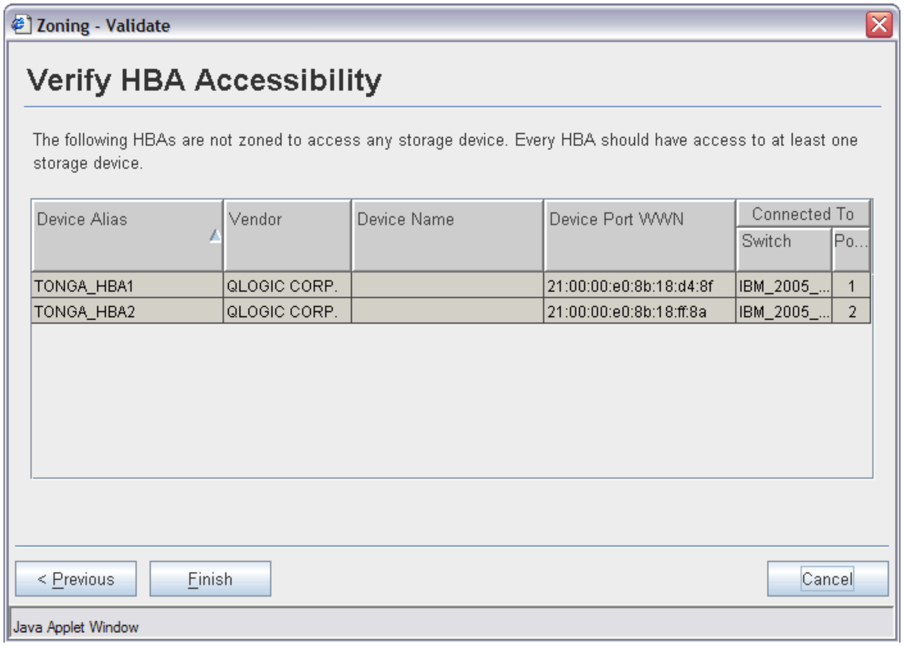


The following storage devices are not zoned for accessibility by any HBA. Every storage device should be accessible by at least one HBA.

Device Alias	Vendor	Device Name	Device Port WWN	Connected To	
				Switch	Po...
DS4400_3	SYMBIOS LOGI...	[28] "IBM 1742 0...	20:06:00:a0:b8:0c:bc:e9	IBM_2005_...	0
DS4400_4	SYMBIOS LOGI...	[28] "IBM 1742 0...	20:07:00:a0:b8:0c:bc:e9	IBM_2005_...	4

Figure 1-40 Verify Storage Accessibility

Clicking **Next** allows us to check the HBA Accessibility as shown in Figure 1-41.

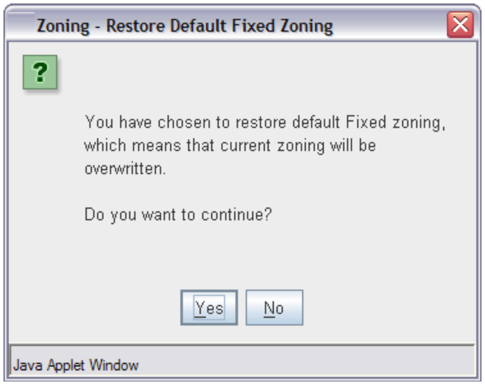

Zoning - Validate
Verify HBA Accessibility
< Previous
Finish
Cancel
Java Applet Window

The following HBAs are not zoned to access any storage device. Every HBA should have access to at least one storage device.

Device Alias	Vendor	Device Name	Device Port WWN	Connected To	
				Switch	Po...
TONGA_HBA1	QLOGIC CORP.		21:00:00:e0:8b:18:d4:8f	IBM_2005_...	1
TONGA_HBA2	QLOGIC CORP.		21:00:00:e0:8b:18:ff:8a	IBM_2005_...	2

Figure 1-41 Verify HBA Accessibility

We can also restore the default fixed zoning from the Zoning menu. Remember that this overwrites the current zoning configuration, and as such, we are requested to confirm before continuing. See Figure 1-42.

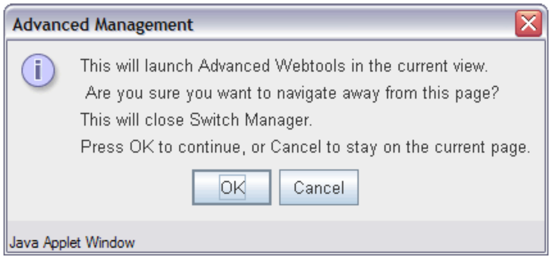

Zoning - Restore Default Fixed Zoning
?
Yes
No
Java Applet Window

You have chosen to restore default Fixed zoning, which means that current zoning will be overwritten.

Do you want to continue?

Figure 1-42 Restore Default Fixed Zoning

To Launch Advanced Webtools, we select Advanced management from the menu. This exits the Switch Manager as detailed in Figure 1-43.



This will launch Advanced Webtools in the current view.
Are you sure you want to navigate away from this page?
This will close Switch Manager.
Press OK to continue, or Cancel to stay on the current page.

Figure 1-43 Launching Advanced Webtools from Switch Manager

Basic troubleshooting with EZSwitchSetup

If reinstallation of EZSwitchSetup or upgrade of EZSwitchSetup fails, we should uninstall the previous version first, then reinstall.

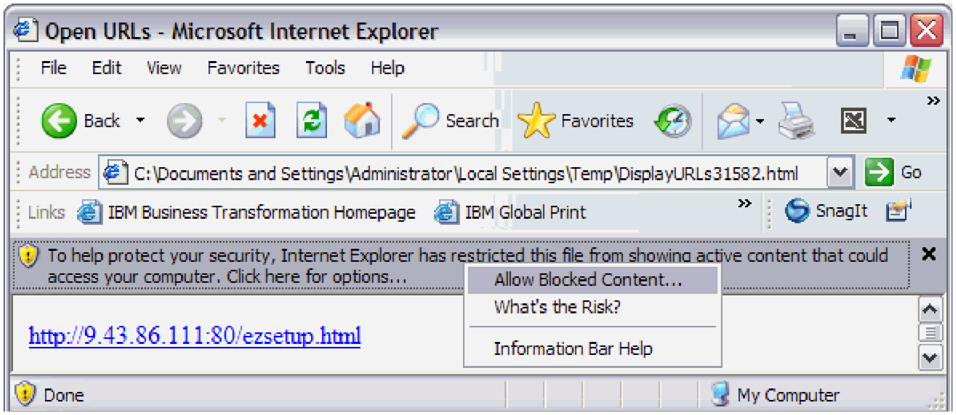
If EZSwitchSetup encounters a launch problem, we should check whether there is already a copy of EZSwitchSetup running on another users machine. Only one copy is allowed to run at any given time.

If during the EZSwitchSetup process, users encounter an operation failure, we should check the serial and Ethernet connection and fix it if necessary, and then re-launch EZSwitchSetup.

If the “Restore Fixed Zoning” action fails, then we have to ensure that the switch has a zoning license installed.

As previously stated, EZSwitchSetup does not fully recognize storage that is presented to the SAN in initiator and target mode. This can happen, for example, if a DS4400 with remote mirroring enabled is connected, as in our examples. Usually we would expect that a simple SAN would not involve this type of configuration, and as such it is unlikely that you will experience this issue. However if you do come across this issue, you can circumvent it by adding only the hosts in the initial setup. You can then add the storage once you have proceeded past the Switch Setup Complete window, as seen in Figure 1-30 on page 74.

After successfully completing the IP address configuration (see Figure 1-22 on page 67) within EZSwitchSetup, you might find that the Switch Configuration window (see Figure 1-23 on page 68) does not open in your browser. In our example, this was caused because the browser was configured to block active content. As such, we selected the **Allow Blocked Content** option from the drop down menu, as detailed in Figure 1-44.


Open URLs - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
Go
Links
IBM Business Transformation Homepage
IBM Global Print
SnagIt
Allow Blocked Content...
What's the Risk?
Information Bar Help
Done
My Computer

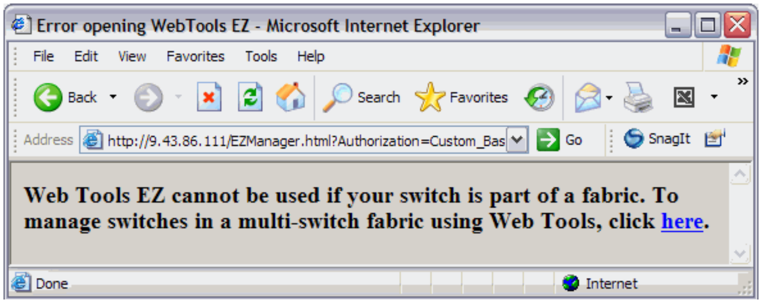
C:\Documents and Settings\Administrator\Local Settings\Temp\DisplayURLs31582.html

To help protect your security, Internet Explorer has restricted this file from showing active content that could access your computer. Click here for options...

http://9.43.86.111:80/ezsetup.html

Figure 1-44 Allowing blocked content in Internet Explorer®

After you have added your switch to a fabric, you are no longer able to access the EZSwitchSetup wizard. This can be seen in Figure 1-45.


Error opening WebTools EZ - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
Go
SnagIt
Done
Internet

http://9.43.86.111/EZManager.html?Authorization=Custom_Bas

Web Tools EZ cannot be used if your switch is part of a fabric. To manage switches in a multi-switch fabric using Web Tools, click here.

Figure 1-45 WebTools EZ error message

1.8 WebTools walk-through

In the following sections, we describe the features of WebTools in more detail. We use both the SAN32B and SAN256B switches to describe the GUI, although the functions are identical on any of the IBM TotalStorage SAN Switch family and equally apply.

The WebTools display has changed significantly since the earlier FOS v3.x or v4.x. We are going to show WebTools using FOS v5.1.0. The tools still have the same basic look and feel to them that they had in previous versions.

WebTools requires any browser that conforms to HTML version 4.0, JavaScript™ version 1.0, and Java plug-in 1.4.2_06 or higher, as in Table 1-10.

Table 1-10 Certified and tested platforms

Operating system	Browser	Java plug-in
Solaris™ 2.8	Mozilla 1.6	1.4.2_06
Solaris 2.9	Mozilla 1.6	1.4.2_06
Windows 2000	Internet Explorer 6.0	1.4.2_06
Windows 2003	Internet Explorer 6.0	1.4.2_06
Windows XP	Internet Explorer 6.0	1.4.2_06

1. Start the Web Browser if it is not already active.
2. Enter the switch name or IP address in the Location/Address field.

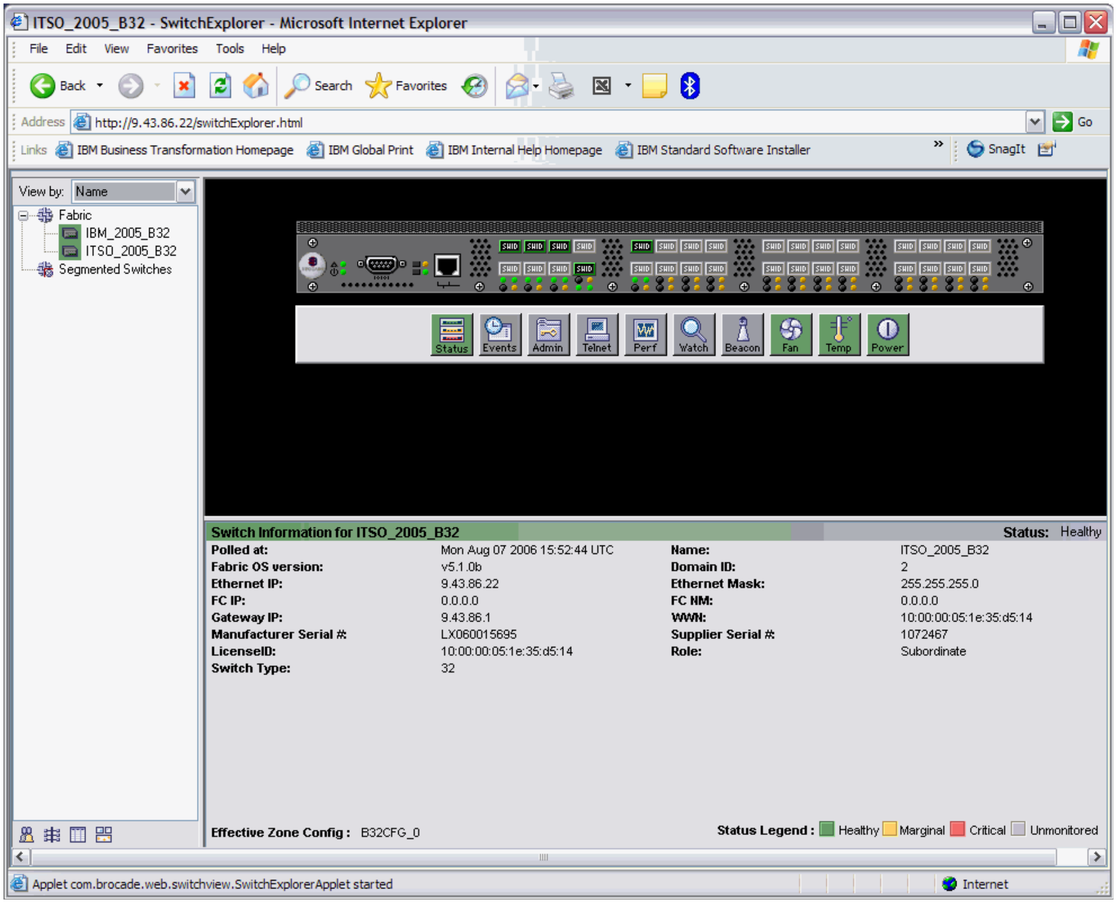
> **Tip:** When managing a multi-switch fabric, we recommend that you enter the *switch name* or IP address of the switch with the largest port count, and the highest *firmware* level.

3. A *Fabric View* appears in the left column, displaying all compatible switches in the fabric. Also, a *Switch View* and details of the switch that we targeted with the IP address are displayed in the larger area on the right side of the browser.

In Figure 1-46, we show the WebTools view window for a dual switch fabric using the SAN32B. It is a feature of WebTools that it displays all interconnected switches within a fabric, and consequently we can see both switches within our fabric.

There are three main components (frames) of the Fabric View window. On the left-hand side is the Fabric Management frame, which includes a list of all the switches in the fabric. At the bottom of the frame are buttons for opening separate Fabric Events, Topology, NameServer, and Zoning windows, shown in Figure 1-47.

The larger two frames display the Switch View and Information View of the switch IP address we pointed our Web browser to. After the initial browser connection to a switch within the fabric, we can select other switch views by clicking the desired switch within the Fabric Frame.


ITSO_2005_B32 - SwitchExplorer - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://9.43.86.22/switchExplorer.html
Go
Links
IBM Business Transformation Homepage
IBM Global Print
IBM Internal Help Homepage
IBM Standard Software Installer
SnagIt
View by:
Name
Fabric
IBM_2005_B32
ITSO_2005_B32
Segmented Switches
Status
Events
Admin
Telnet
Perf
Watch
Beacon
Fan
Temp
Power
Applet com.brocade.web.switchview.SwitchExplorerApplet started
Internet

Switch Information for ITSO_2005_B32 **Status:** Healthy

Polled at:	Mon Aug 07 2006 15:52:44 UTC	**Name:**	ITSO_2005_B32
Fabric OS version:	v5.1.0b	**Domain ID:**	2
Ethernet IP:	9.43.86.22	**Ethernet Mask:**	255.255.255.0
FC IP:	0.0.0.0	**FC NM:**	0.0.0.0
Gateway IP:	9.43.86.1	**WWN:**	10:00:00:05:1e:35:d5:14
Manufacturer Serial #:	LX060015695	**Supplier Serial #:**	1072467
LicenseID:	10:00:00:05:1e:35:d5:14	**Role:**	Subordinate
Switch Type:	32		

Effective Zone Config : B32CFG_0

Status Legend : 🟩 Healthy 🟨 Marginal 🟥 Critical ☐ Unmonitored

Figure 1-46 B32 WebTools main screen

Figure 1-47 shows the various buttons for opening separate Fabric Events, Topology, NameServer, and Zoning windows. As the mouse hovers across each of these, you see them highlighted, and a description of the item is presented in the command line region at the bottom left hand side of the main SwitchExplorer window.

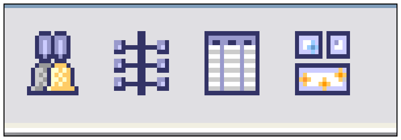
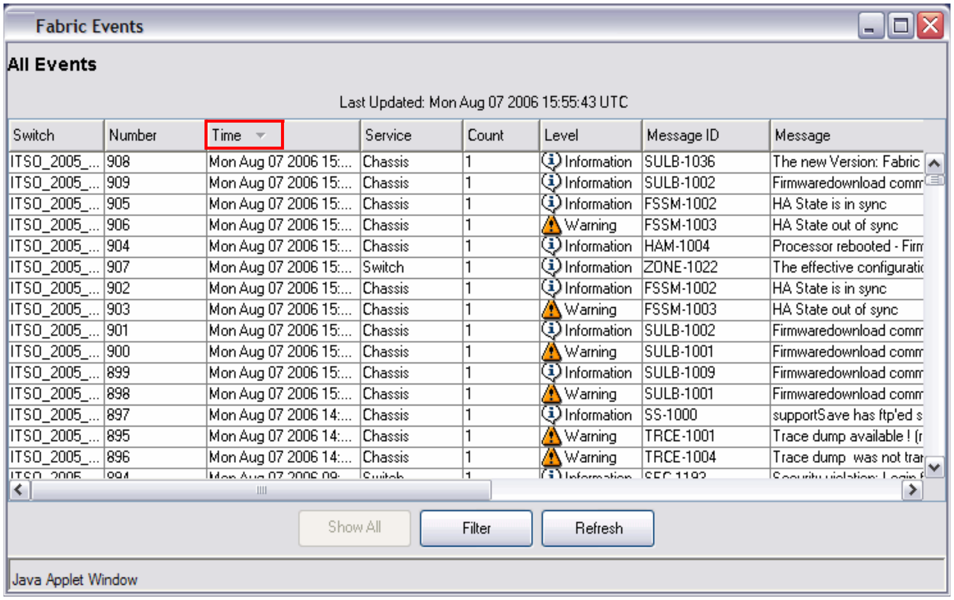


Figure 1-47 Fabric Events, Topology, Name Server, and Zone Admin buttons

1.8.1 Fabric Events icon

Fabric Events is a log of all the events that have occurred across the fabric. The Fabric Watch conditions are logged as well as other Fabric-wide events. In Figure 1-48, we have launched the Fabric Events log for our SAN32B switch.



Last Updated: Mon Aug 07 2006 15:55:43 UTC

Switch	Number	Time	Service	Count	Level	Message ID	Message
ITSO_2005_...	908	Mon Aug 07 2006 15:...	Chassis	1	Information	SULB-1036	The new Version: Fabric
ITSO_2005_...	909	Mon Aug 07 2006 15:...	Chassis	1	Information	SULB-1002	Firmwaredownload comm
ITSO_2005_...	905	Mon Aug 07 2006 15:...	Chassis	1	Information	FSSM-1002	HA State is in sync
ITSO_2005_...	906	Mon Aug 07 2006 15:...	Chassis	1	Warning	FSSM-1003	HA State out of sync
ITSO_2005_...	904	Mon Aug 07 2006 15:...	Chassis	1	Information	HAM-1004	Processor rebooted - Firm
ITSO_2005_...	907	Mon Aug 07 2006 15:...	Switch	1	Information	ZONE-1022	The effective configurati
ITSO_2005_...	902	Mon Aug 07 2006 15:...	Chassis	1	Information	FSSM-1002	HA State is in sync
ITSO_2005_...	903	Mon Aug 07 2006 15:...	Chassis	1	Warning	FSSM-1003	HA State out of sync
ITSO_2005_...	901	Mon Aug 07 2006 15:...	Chassis	1	Information	SULB-1002	Firmwaredownload comm
ITSO_2005_...	900	Mon Aug 07 2006 15:...	Chassis	1	Warning	SULB-1001	Firmwaredownload comm
ITSO_2005_...	899	Mon Aug 07 2006 15:...	Chassis	1	Information	SULB-1009	Firmwaredownload comm
ITSO_2005_...	898	Mon Aug 07 2006 15:...	Chassis	1	Warning	SULB-1001	Firmwaredownload comm
ITSO_2005_...	897	Mon Aug 07 2006 14:...	Chassis	1	Information	SS-1000	supportSave has ftp'ed s
ITSO_2005_...	895	Mon Aug 07 2006 14:...	Chassis	1	Warning	TRCE-1001	Trace dump available ! (r
ITSO_2005_...	896	Mon Aug 07 2006 14:...	Chassis	1	Warning	TRCE-1004	Trace dump was not tra
ITSO_2005_...	894	Mon Aug 07 2006 09:...	Switch	1	Information	SEC-1193	Security violation: Login f

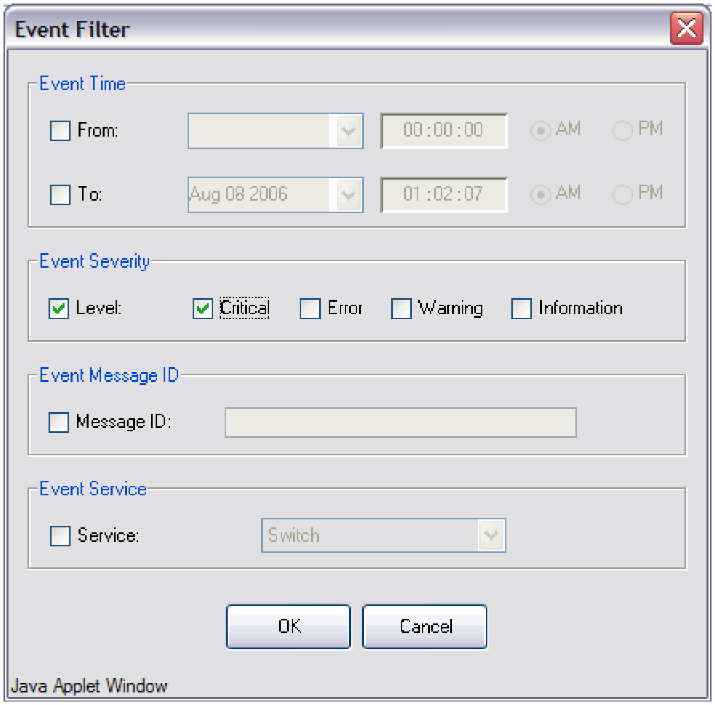
Figure 1-48 SAN32B Fabric Events

We can sort the columns into ascending or descending order by clicking the column headings; in our example we have sorted by time, indicated by the small arrow head in the *Time* column heading. We can also rearrange the columns to suit our requirements by dragging and dropping them as required. Table 1-11 explains the Fabric Events log.

Table 1-11 Fabric Events log details

Field name	Description
Switch	Name of switch for which events occurred
Number	Order number of when event occurred, most current at top
Time	Date and time stamp of message
Service	Which service part of switch encountered an error
Count	Number of times this error occurred
Level	Whether message is informational, warning, or error
Message ID	Message ID number
Message	One line detailed description of the message

We can also filter the log by clicking the **Filter** button and selecting the appropriate choices as shown in Figure 1-49.


Event Filter

Event Time
☐ From: 00 : 00 : 00 ● AM ○ PM
☐ To: Aug 08 2006 01 : 02 : 07 ● AM ○ PM

Event Severity
☑ Level: ☑ Critical ☐ Error ☐ Warning ☐ Information

Event Message ID
☐ Message ID:

Event Service
☐ Service: Switch

Figure 1-49 Filtering the Event Log

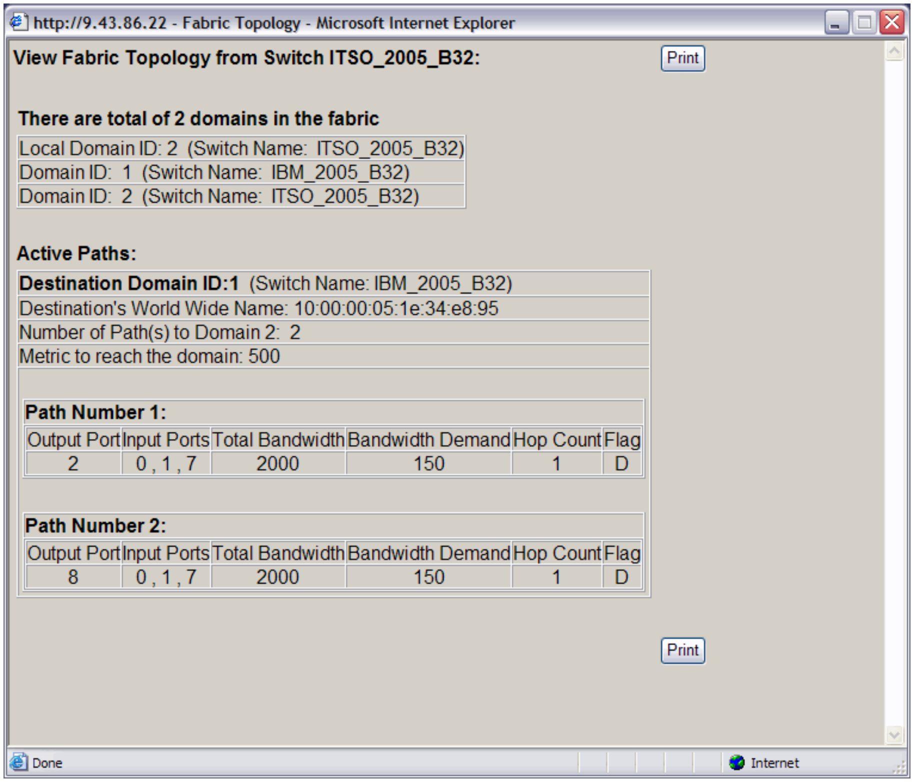
When analysis is complete, to exit from the log, just close the window.

1.8.2 Topology icon

The *topology* is the physical configuration of the fabric, including active domains and paths. The topology report is as viewed from the local domain (the local domain is the switch that was selected in the fabric view frame).

Clicking the second button from the left as shown in Figure 1-47 on page 88 takes us to the Fabric Topology report shown in Figure 1-50 on page 92.

For our purposes, we have shown a topology with two switches.


http://9.43.86.22 - Fabric Topology - Microsoft Internet Explorer
Print
Print
Done
Internet

View Fabric Topology from Switch ITSO_2005_B32:

There are total of 2 domains in the fabric

Local Domain ID: 2 (Switch Name: ITSO_2005_B32)
Domain ID: 1 (Switch Name: IBM_2005_B32)
Domain ID: 2 (Switch Name: ITSO_2005_B32)

Active Paths:

Destination Domain ID:1 (Switch Name: IBM_2005_B32)
Destination's World Wide Name: 10:00:00:05:1e:34:e8:95
Number of Path(s) to Domain 2: 2
Metric to reach the domain: 500

Path Number 1:

Output Port	Input Ports	Total Bandwidth	Bandwidth Demand	Hop Count	Flag
2	0 , 1 , 7	2000	150	1	D

Path Number 2:

Output Port	Input Ports	Total Bandwidth	Bandwidth Demand	Hop Count	Flag
8	0 , 1 , 7	2000	150	1	D

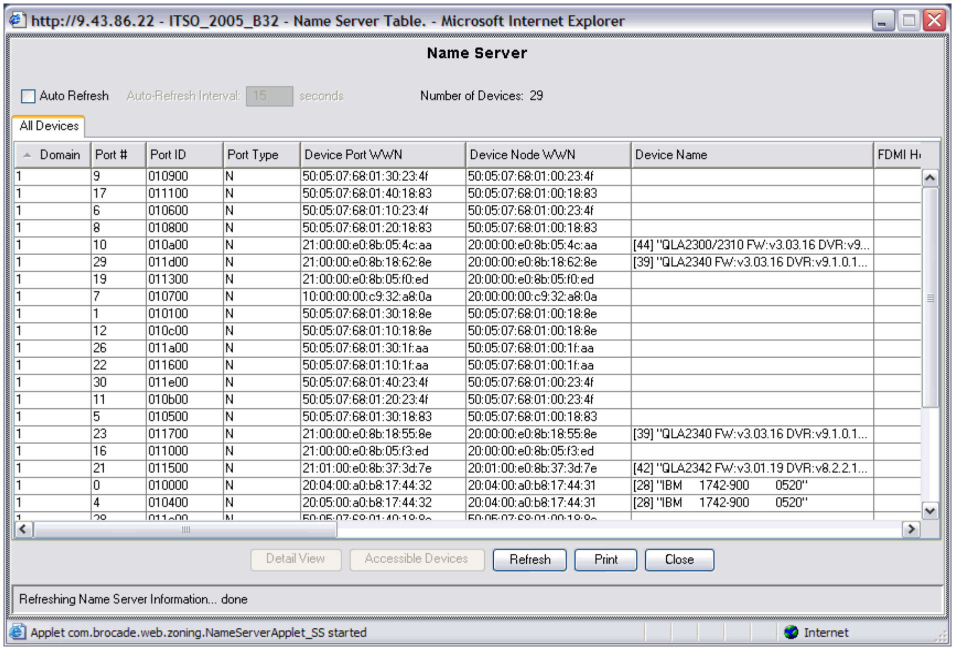
Figure 1-50 Fabric Topology Report

The Fabric Topology report lists the domain IDs and switch names for all the active domains in the fabric.

For each switch in the fabric, the window displays the active paths to the local domain (these are the Inter-Switch Links (ISLs). Also shown are the output port numbers (ISL ports), input port numbers, and the hop count.

1.8.3 Name Server icon

The Name Server table provides the Name Server entries listed in the name server database as shown in Figure 1-51. This includes all name server entries for the fabric, not only those local to the host domain. Each row in the table represents a different device which has logged into the fabric. The Name Server table provides a good cross reference of WWPN / WWN and the port position on the switch. It also lists the zones that the port is a member of, and therefore can be a very useful problem determination tool.


http://9.43.86.22 - ITSO_2005_B32 - Name Server Table. - Microsoft Internet Explorer
Name Server
☐ Auto Refresh
Auto-Refresh Interval: 15 seconds
All Devices
Detail View
Accessible Devices
Refresh
Print
Close
Internet

Number of Devices: 29

Domain	Port #	Port ID	Port Type	Device Port WWN	Device Node WWN	Device Name	FDMI H
1	9	010900	N	50:05:07:68:01:30:23:4f	50:05:07:68:01:00:23:4f		
1	17	011100	N	50:05:07:68:01:40:18:83	50:05:07:68:01:00:18:83		
1	6	010600	N	50:05:07:68:01:10:23:4f	50:05:07:68:01:00:23:4f		
1	8	010800	N	50:05:07:68:01:20:18:83	50:05:07:68:01:00:18:83		
1	10	010a00	N	21:00:00:e0:8b:05:4c:aa	20:00:00:e0:8b:05:4c:aa	[44] "QLA2300/2310 FW:v3.03.16 DVR:v9...	
1	29	011d00	N	21:00:00:e0:8b:18:62:8e	20:00:00:e0:8b:18:62:8e	[39] "QLA2340 FW:v3.03.16 DVR:v9.1.0.1...	
1	19	011300	N	21:00:00:e0:8b:05:f0:ed	20:00:00:e0:8b:05:f0:ed		
1	7	010700	N	10:00:00:00:c9:32:a8:0a	20:00:00:00:c9:32:a8:0a		
1	1	010100	N	50:05:07:68:01:30:18:8e	50:05:07:68:01:00:18:8e		
1	12	010c00	N	50:05:07:68:01:10:18:8e	50:05:07:68:01:00:18:8e		
1	26	011a00	N	50:05:07:68:01:30:1f:aa	50:05:07:68:01:00:1f:aa		
1	22	011600	N	50:05:07:68:01:10:1f:aa	50:05:07:68:01:00:1f:aa		
1	30	011e00	N	50:05:07:68:01:40:23:4f	50:05:07:68:01:00:23:4f		
1	11	010b00	N	50:05:07:68:01:20:23:4f	50:05:07:68:01:00:23:4f		
1	5	010500	N	50:05:07:68:01:30:18:83	50:05:07:68:01:00:18:83		
1	23	011700	N	21:00:00:e0:8b:18:55:8e	20:00:00:e0:8b:18:55:8e	[39] "QLA2340 FW:v3.03.16 DVR:v9.1.0.1...	
1	16	011000	N	21:00:00:e0:8b:05:f3:ed	20:00:00:e0:8b:05:f3:ed		
1	21	011500	N	21:01:00:e0:8b:37:3d:7e	20:01:00:e0:8b:37:3d:7e	[42] "QLA2342 FW:v3.01.19 DVR:v8.2.2.1...	
1	0	010000	N	20:04:00:a0:b8:17:44:32	20:04:00:a0:b8:17:44:31	[28] "IBM 1742-900 0520"	
1	4	010400	N	20:05:00:a0:b8:17:44:32	20:04:00:a0:b8:17:44:31	[28] "IBM 1742-900 0520"	

Refreshing Name Server Information... done

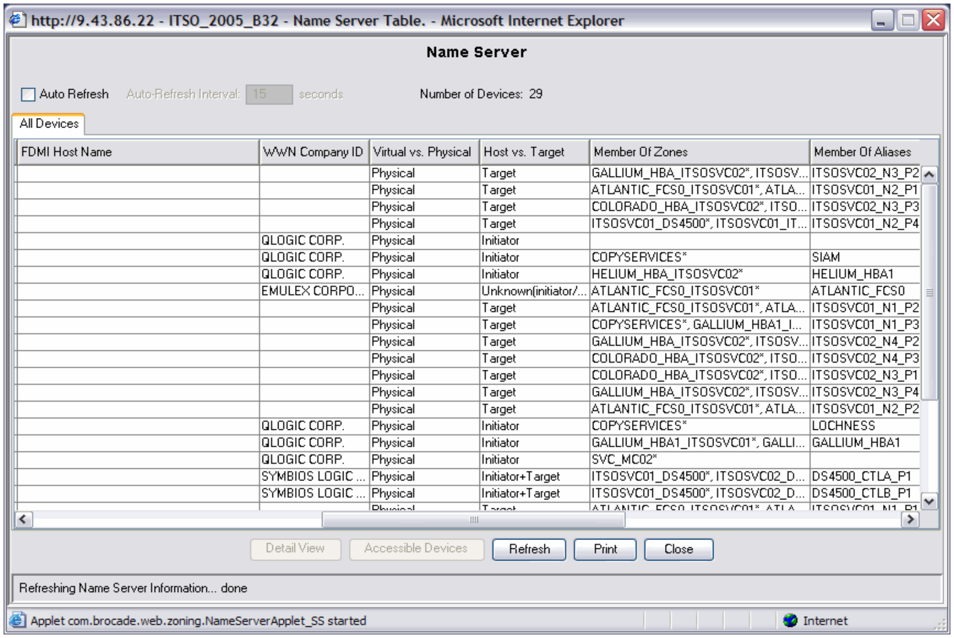
Applet com.brocade.web.zoning.NameServerApplet_SS started

Figure 1-51 SAN32B Nameserver table part 1 of 3

The Name Server table contains the following parameters:

Domain	Domain ID of the switch to which the device is connected
Port #	Port number of the switch to which the device is connected
Port ID	The Fibre Channel Port address of the device (basically, a 24-bit hexadecimal number)
Port Type	Shows whether the port is a public loop port (NL) or whether it is a normal switch fabric port (N)
Device Port WWN	World-wide name for the device port (WWPN)
Device Node WWN	World-wide name of the device node (WWNN)
Device Name	Name of the device according to the SCSI INQUIRY such as FCP or IP

Scrolling to the right, as shown below in Figure 1-52 and Figure 1-53, we are able to see the rest of the parameters that are available.



http://9.43.86.22 - ITSO_2005_B32 - Name Server Table. - Microsoft Internet Explorer
Name Server
All Devices
Detail View
Accessible Devices
Refresh
Print
Close
Internet

☐ Auto Refresh Auto-Refresh Interval: 15 seconds Number of Devices: 29

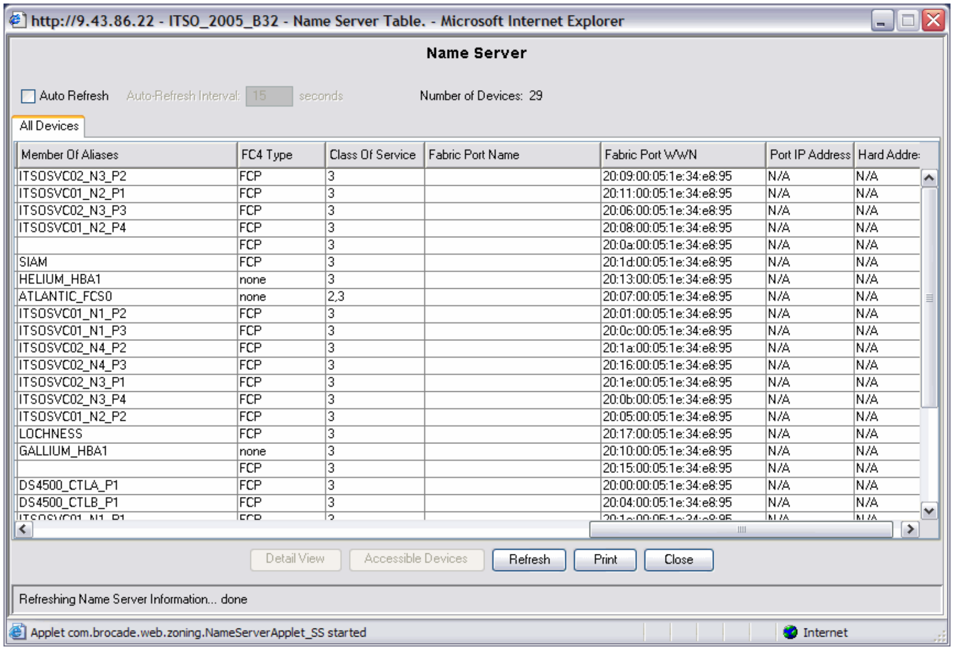
FDMI Host Name	WWN Company ID	Virtual vs. Physical	Host vs. Target	Member Of Zones	Member Of Aliases
		Physical	Target	GALLIUM_HBA_ITSOSVC02*, ITSOSV...	ITSOSVC02_N3_P2
		Physical	Target	ATLANTIC_FCS0_ITSOSVC01*, ATLA...	ITSOSVC01_N2_P1
		Physical	Target	COLORADO_HBA_ITSOSVC02*, ITSO...	ITSOSVC02_N3_P3
		Physical	Target	ITSOSVC01_DS4500*, ITSOSVC01_IT...	ITSOSVC01_N2_P4
	QLOGIC CORP.	Physical	Initiator		
	QLOGIC CORP.	Physical	Initiator	COPYSERVICES*	SIAM
	QLOGIC CORP.	Physical	Initiator	HELIUM_HBA_ITSOSVC02*	HELIUM_HBA1
	EMULEX CORPO...	Physical	Unknown(initiator/...	ATLANTIC_FCS0_ITSOSVC01*	ATLANTIC_FCS0
		Physical	Target	ATLANTIC_FCS0_ITSOSVC01*, ATLA...	ITSOSVC01_N1_P2
		Physical	Target	COPYSERVICES*, GALLIUM_HBA1_I...	ITSOSVC01_N1_P3
		Physical	Target	GALLIUM_HBA_ITSOSVC02*, ITSOSV...	ITSOSVC02_N4_P2
		Physical	Target	COLORADO_HBA_ITSOSVC02*, ITSO...	ITSOSVC02_N4_P3
		Physical	Target	COLORADO_HBA_ITSOSVC02*, ITSO...	ITSOSVC02_N3_P1
		Physical	Target	GALLIUM_HBA_ITSOSVC02*, ITSOSV...	ITSOSVC02_N3_P4
		Physical	Target	ATLANTIC_FCS0_ITSOSVC01*, ATLA...	ITSOSVC01_N2_P2
	QLOGIC CORP.	Physical	Initiator	COPYSERVICES*	LOCHNESS
	QLOGIC CORP.	Physical	Initiator	GALLIUM_HBA1_ITSOSVC01*, GALLI...	GALLIUM_HBA1
	QLOGIC CORP.	Physical	Initiator	SVC_MC02*	
	SYMBIOS LOGIC ...	Physical	Initiator+Target	ITSOSVC01_DS4500*, ITSOSVC02_D...	DS4500_CTLA_P1
	SYMBIOS LOGIC ...	Physical	Initiator+Target	ITSOSVC01_DS4500*, ITSOSVC02_D...	DS4500_CTLB_P1

Refreshing Name Server Information... done

Applet com.brocade.web.zoning.NameServerApplet_SS started

Figure 1-52 SAN32B Name Server table part 2 of 3

FDMI Host Name	Displays the FDMI host name of the device
WWN Company ID	Displays vendor company based on device WWN
Virtual vs. Physical	Identifies type of device, virtual or physical
Host vs. Target	Identifies type of device, host or target
Member of Zones	List of zones to which the device belongs
Member of Aliases	List of aliases for this device


http://9.43.86.22 - ITSO_2005_B32 - Name Server Table. - Microsoft Internet Explorer
Name Server
☐ Auto Refresh
Auto-Refresh Interval: 15 seconds
Number of Devices: 29
All Devices

Member Of Aliases	FC4 Type	Class Of Service	Fabric Port Name	Fabric Port WWN	Port IP Address	Hard Addre
ITSOSVC02_N3_P2	FCP	3		20:09:00:05:1e:34:e8:95	N/A	N/A
ITSOSVC01_N2_P1	FCP	3		20:11:00:05:1e:34:e8:95	N/A	N/A
ITSOSVC02_N3_P3	FCP	3		20:06:00:05:1e:34:e8:95	N/A	N/A
ITSOSVC01_N2_P4	FCP	3		20:08:00:05:1e:34:e8:95	N/A	N/A
	FCP	3		20:0a:00:05:1e:34:e8:95	N/A	N/A
SIAM	FCP	3		20:1d:00:05:1e:34:e8:95	N/A	N/A
HELIUM_HBA1	none	3		20:13:00:05:1e:34:e8:95	N/A	N/A
ATLANTIC_FCS0	none	2,3		20:07:00:05:1e:34:e8:95	N/A	N/A
ITSOSVC01_N1_P2	FCP	3		20:01:00:05:1e:34:e8:95	N/A	N/A
ITSOSVC01_N1_P3	FCP	3		20:0c:00:05:1e:34:e8:95	N/A	N/A
ITSOSVC02_N4_P2	FCP	3		20:1a:00:05:1e:34:e8:95	N/A	N/A
ITSOSVC02_N4_P3	FCP	3		20:16:00:05:1e:34:e8:95	N/A	N/A
ITSOSVC02_N3_P1	FCP	3		20:1e:00:05:1e:34:e8:95	N/A	N/A
ITSOSVC02_N3_P4	FCP	3		20:0b:00:05:1e:34:e8:95	N/A	N/A
ITSOSVC01_N2_P2	FCP	3		20:05:00:05:1e:34:e8:95	N/A	N/A
LOCHNESS	FCP	3		20:17:00:05:1e:34:e8:95	N/A	N/A
GALLIUM_HBA1	none	3		20:10:00:05:1e:34:e8:95	N/A	N/A
	FCP	3		20:15:00:05:1e:34:e8:95	N/A	N/A
DS4500_CTLA_P1	FCP	3		20:00:00:05:1e:34:e8:95	N/A	N/A
DS4500_CTLB_P1	FCP	3		20:04:00:05:1e:34:e8:95	N/A	N/A

Detail View
Accessible Devices
Refresh
Print
Close

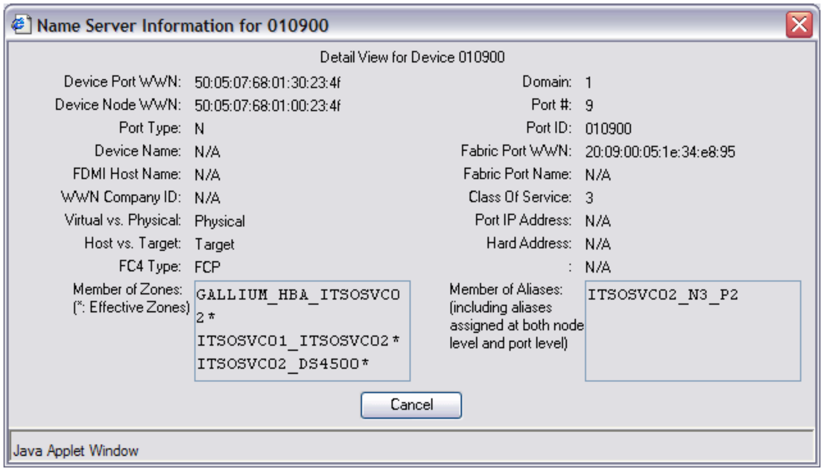
Refreshing Name Server Information... done

Applet com.brocade.web.zoning.NameServerApplet_SS started

Figure 1-53 SAN32B Name Server table part 3 of 3

FC4 Type	Fibre Channel FC4 layer types supported by device, such as FCP or IP
Class of Service	Class of service that the device supports
Fabric Port Name	Displays the name of the port
Fabric Port WWN	The worldwide name of the fabric port
Port IP Address	IP address of the fabric port (might be zeroes)
Hard Address	Hard address assigned to the fabric port

To view all of the details for a given device in the Name Server table, we highlight the device we are interested in. Next, we click the **Detail View** button. This brings up the Detailed View window as seen in Figure 1-54.



Detail View for Device 010900

Device Port WWN: 50:05:07:68:01:30:23:4f
Device Node WWN: 50:05:07:68:01:00:23:4f
Port Type: N
Device Name: N/A
FDMI Host Name: N/A
WWN Company ID: N/A
Virtual vs. Physical: Physical
Host vs. Target: Target
FC4 Type: FCP
Member of Zones: (*: Effective Zones) GALLIUM_HBA_ITSOSVC02* ITSOSVC01_ITSOSVC02* ITSOSVC02_DS4500*

Domain: 1
Port #: 9
Port ID: 010900
Fabric Port WWN: 20:09:00:05:1e:34:e8:95
Fabric Port Name: N/A
Class Of Service: 3
Port IP Address: N/A
Hard Address: N/A
: N/A
Member of Aliases: (including aliases assigned at both node level and port level) ITSOSVC02_N3_P2

Figure 1-54 SAN32B Name server Detailed view

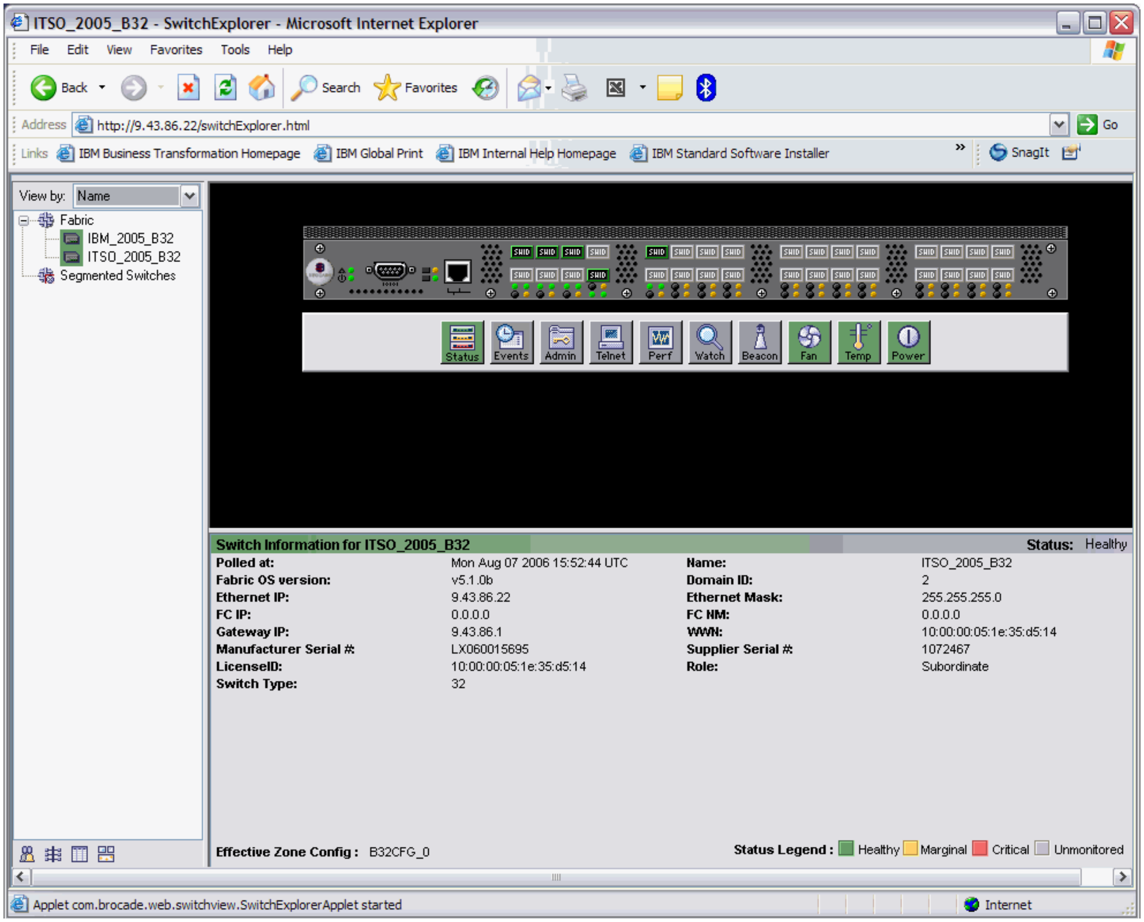
1.8.4 Zoning icon

We describe the functionality behind this button within the zoning section of this chapter; see 1.9.9, “Zoning” on page 291.

1.8.5 Main view

From the Switch View of WebTools, we can view the status of the individual switch, firmware version, IP addresses, port state, and see if there are any out-of-line events.

The Switch View presents a picture of the switch as shown in Figure 1-55.


ITSO_2005_B32 - SwitchExplorer - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://9.43.86.22/switchExplorer.html
Go
Links IBM Business Transformation Homepage IBM Global Print IBM Internal Help Homepage IBM Standard Software Installer
SnagIt
View by: Name
Fabric
IBM_2005_B32
ITSO_2005_B32
Segmented Switches
Status
Events
Admin
Telnet
Perf
Watch
Beacon
Fan
Temp
Power
Applet com.brocade.web.switchview.SwitchExplorerApplet started
Internet

Switch Information for ITSO_2005_B32 **Status:** Healthy

Polled at: Mon Aug 07 2006 15:52:44 UTC
Fabric OS version: v5.1.0b
Ethernet IP: 9.43.86.22
FC IP: 0.0.0.0
Gateway IP: 9.43.86.1
Manufacturer Serial #: LX060015695
LicenseID: 10:00:00:05:1e:35:d5:14
Switch Type: 32
Name: ITSO_2005_B32
Domain ID: 2
Ethernet Mask: 255.255.255.0
FC NM: 0.0.0.0
WWN: 10:00:00:05:1e:35:d5:14
Supplier Serial #: 1072467
Role: Subordinate

Effective Zone Config : B32CFG_0

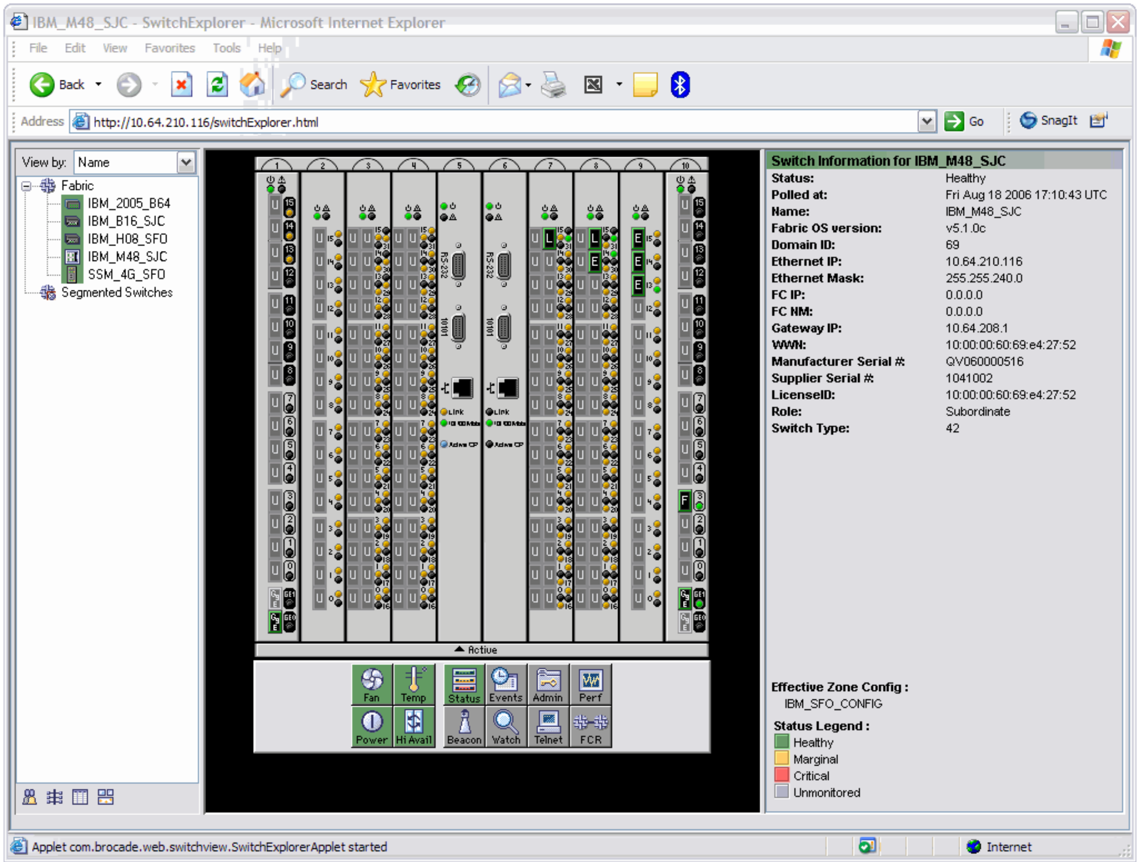
Status Legend : 🟩 Healthy 🟨 Marginal 🟥 Critical ☐ Unmonitored

Figure 1-55 SAN32B switch view from WebTools

From this view, we also have an overview of the actual switch front panel and monitor LEDs.

There are buttons that allow us to drill down further into the switch. We can select to view status of the switch, display switch events, complete administrative duties, open a telnet session, run performance testing, as well as check the fans. switch temperature, and power.

Next we point our browser to the IP address of a SAN256B as shown in Figure 1-56. Here we can see its detailed information, which would be similar for the other models.


IBM_M48_SJC - SwitchExplorer - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://10.64.210.116/switchExplorer.html
Go
SnagIt
View by: Name
Fabric
IBM_2005_B64
IBM_B16_SJC
IBM_H08_SFO
IBM_M48_SJC
SSM_4G_SFO
Segmented Switches
Active
Fan
Temp
Status
Events
Admin
Perf
Power
Hi Avail
Beacon
Watch
Telnet
FCR
Applet com.brocade.web.switchview.SwitchExplorerApplet started
Internet

Switch Information for IBM_M48_SJC

Status:	Healthy
Polled at:	Fri Aug 18 2006 17:10:43 UTC
Name:	IBM_M48_SJC
Fabric OS version:	v5.1.0c
Domain ID:	69
Ethernet IP:	10.64.210.116
Ethernet Mask:	255.255.240.0
FC IP:	0.0.0.0
FC NM:	0.0.0.0
Gateway IP:	10.64.208.1
WWN:	10:00:00:60:69:e4:27:52
Manufacturer Serial #:	QV060000516
Supplier Serial #:	1041002
LicenseID:	10:00:00:60:69:e4:27:52
Role:	Subordinate
Switch Type:	42

Effective Zone Config :
IBM_SFO_CONFIG

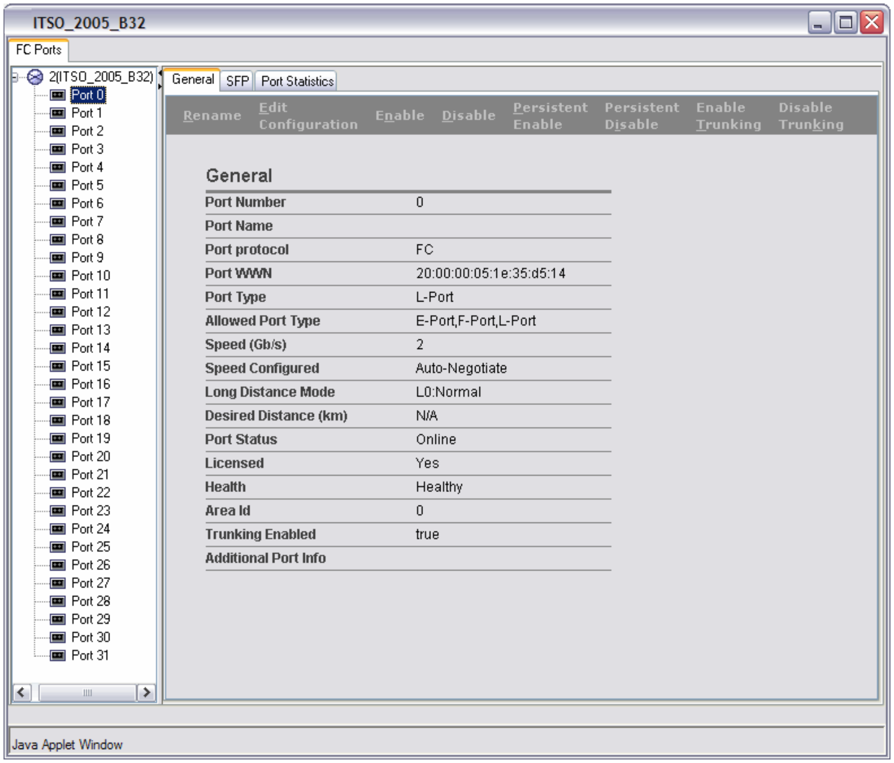
Status Legend :
🟩 Healthy
🟨 Marginal
🟥 Critical
⬜ Unmonitored

Figure 1-56 M48 switch view from WebTools

From the M48 Switch view, we can also look at temperature, fan speeds, CP status, and power supply status for the overall chassis.

1.8.6 Port information

To access the detailed port information, click the appropriate port. The port information is displayed for the switch as shown in Figure 1-57.


ITSO_2005_B32
FC Ports
2(ITSO_2005_B32)
Port 0
Port 1
Port 2
Port 3
Port 4
Port 5
Port 6
Port 7
Port 8
Port 9
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15
Port 16
Port 17
Port 18
Port 19
Port 20
Port 21
Port 22
Port 23
Port 24
Port 25
Port 26
Port 27
Port 28
Port 29
Port 30
Port 31
General
SFP
Port Statistics
Rename
Edit Configuration
Enable
Disable
Persistent Enable
Persistent Disable
Enable Trunking
Disable Trunking
Java Applet Window

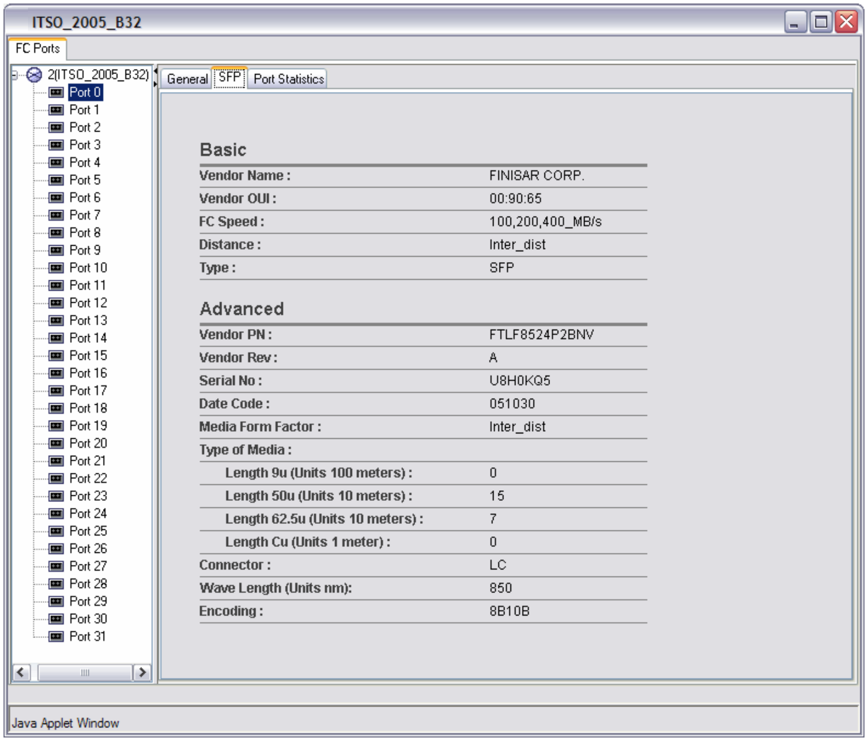
General

Port Number	0
Port Name	
Port protocol	FC
Port WWN	20:00:00:05:1e:35:d5:14
Port Type	L-Port
Allowed Port Type	E-Port,F-Port,L-Port
Speed (Gb/s)	2
Speed Configured	Auto-Negotiate
Long Distance Mode	L0:Normal
Desired Distance (km)	N/A
Port Status	Online
Licensed	Yes
Health	Healthy
Area Id	0
Trunking Enabled	true
Additional Port Info	

Figure 1-57 SAN32B single port details from WebTools

From this window, we can select any of the switch ports. If an SFP is installed, then additional information on the SFP itself can be selected by accessing the **SFP** tab as displayed in Figure 1-58. The **Port statistics** tab is displayed in Figure 1-59.

> **Note:** As we are not logged in to an account on the switch at this stage, we can only view the port information and not edit it. If you want to edit the port information, this can be done by selecting the **Ports** tab within the Admin tool; refer to the “Ports tab” on page 148.


ITSO_2005_B32
FC Ports
2(ITSO_2005_B32)
Port 0
Port 1
Port 2
Port 3
Port 4
Port 5
Port 6
Port 7
Port 8
Port 9
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15
Port 16
Port 17
Port 18
Port 19
Port 20
Port 21
Port 22
Port 23
Port 24
Port 25
Port 26
Port 27
Port 28
Port 29
Port 30
Port 31
General
SFP
Port Statistics
Java Applet Window

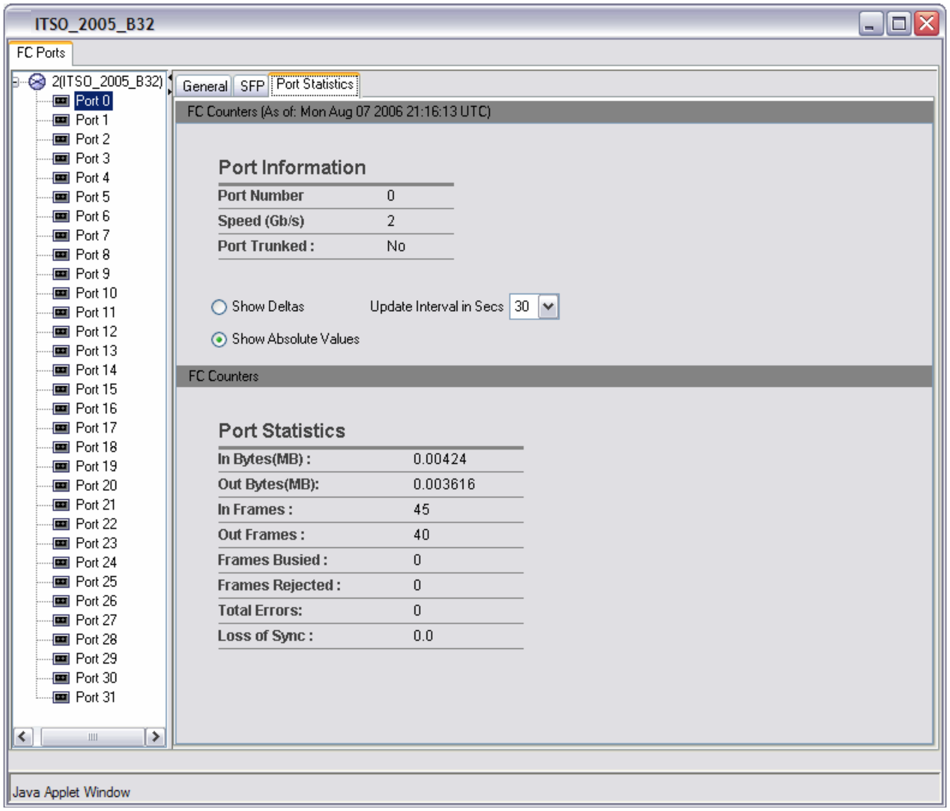
Basic

Vendor Name :	FINISAR CORP.
Vendor OUI :	00:90:65
FC Speed :	100,200,400_MB/s
Distance :	Inter_dist
Type :	SFP

Advanced

Vendor PN :	FTLF8524P2BNV
Vendor Rev :	A
Serial No :	U8H0KQ5
Date Code :	051030
Media Form Factor :	Inter_dist
Type of Media :	
Length 9u (Units 100 meters) :	0
Length 50u (Units 10 meters) :	15
Length 62.5u (Units 10 meters) :	7
Length Cu (Units 1 meter) :	0
Connector :	LC
Wave Length (Units nm):	850
Encoding :	8B10B

Figure 1-58 SAN32B SFP view from WebTools


ITSO_2005_B32
FC Ports
2(ITSO_2005_B32)
Port 0
Port 1
Port 2
Port 3
Port 4
Port 5
Port 6
Port 7
Port 8
Port 9
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15
Port 16
Port 17
Port 18
Port 19
Port 20
Port 21
Port 22
Port 23
Port 24
Port 25
Port 26
Port 27
Port 28
Port 29
Port 30
Port 31
General
SFP
Port Statistics
Java Applet Window

FC Counters (As of: Mon Aug 07 2006 21:16:13 UTC)

Port Information

Port Number	0
Speed (Gb/s)	2
Port Trunked :	No

○ Show Deltas   Update Interval in Secs 30

● Show Absolute Values

FC Counters

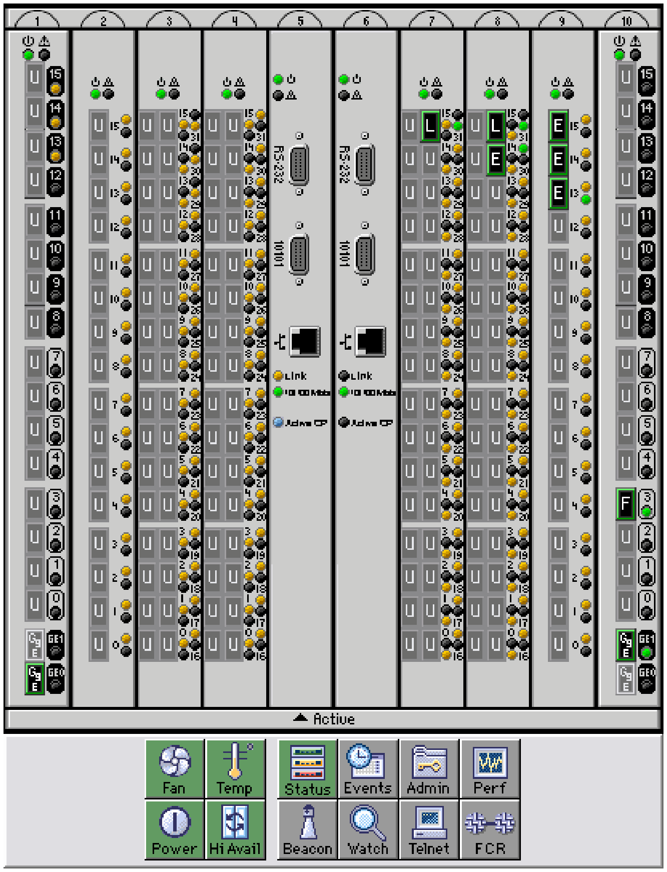
Port Statistics

In Bytes(MB) :	0.00424
Out Bytes(MB):	0.003616
In Frames :	45
Out Frames :	40
Frames Busied :	0
Frames Rejected :	0
Total Errors:	0
Loss of Sync :	0.0

Figure 1-59 SAN32B single port statistics from WebTools

Port information for the M48

The graphical representation of the physical M48 chassis, in the middle of the frame, is shown in Figure 1-60.



1
2
3
4
5
6
7
8
9
10
RS-232
10101
Link
10/100 Mbit
Active CP
Active
Fan
Temp
Status
Events
Admin
Perf
Power
Hi Avail
Beacon
Watch
Telnet
FCR

Figure 1-60 2109-M48 ports view from WebTools

This view shows only the physically installed port blades for each switch, plus the utility icons. We have four FC4-32 port blades in slots 3,4,7 and 8, plus two FC4-16 port blades in slots 2 and 9, with two FR4-18i routing blades in slots 1 and 10. The Active CP is also indicated by the arrow below it.

Double-clicking a particular port gives us a view of the detailed information for that port as we saw with the SAN32B example in Figure 1-59 on page 101. However, we also have the ability to select the particular FC port card slot and GE ports as shown in Figure 1-61.

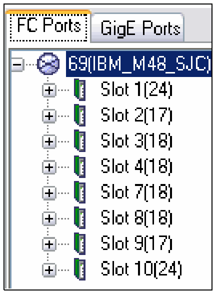

FC Ports
GigE Ports
69(IBM_M48_SJC)
Slot 1(24)
Slot 2(17)
Slot 3(18)
Slot 4(18)
Slot 7(18)
Slot 8(18)
Slot 9(17)
Slot 10(24)

Figure 1-61 M48 specific ports view

Other information from the switch view is available by clicking the appropriate button at the bottom of the view, as shown in Figure 1-62.

While most of these buttons perform the same function on all switches, we have displayed those on the SAN256B, because this model has additional features, **`Hi Avail`** and **`FCR`**, that are not present on all of the b-type family switches.

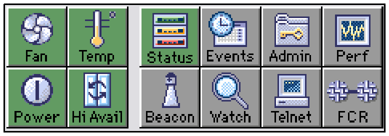
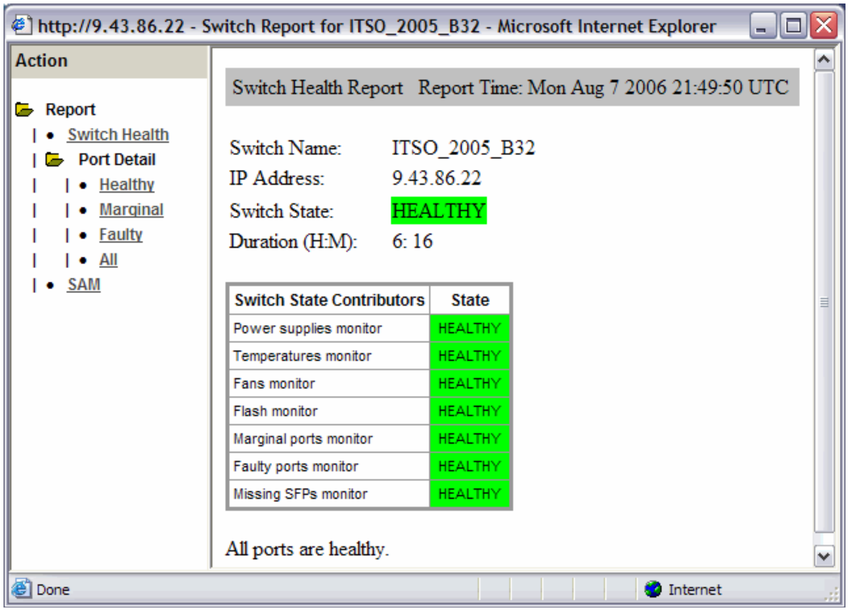

Fan
Temp
Status
Events
Admin
Perf
Power
Hi Avail
Beacon
Watch
Telnet
FCR

Figure 1-62 M48 switch view showing the master buttons from WebTools

1.8.7 Status button

The Status button is available on all IBM TotalStorage SAN Switch models. Clicking the **Status** button brings up the Switch Health Report window showing you the health of the switch, as shown in Figure 1-63.


http://9.43.86.22 - Switch Report for ITSO_2005_B32 - Microsoft Internet Explorer
Action
Report
Switch Health
Port Detail
Healthy
Marginal
Faulty
All
SAM
Done
Internet

Switch Health Report Report Time: Mon Aug 7 2006 21:49:50 UTC

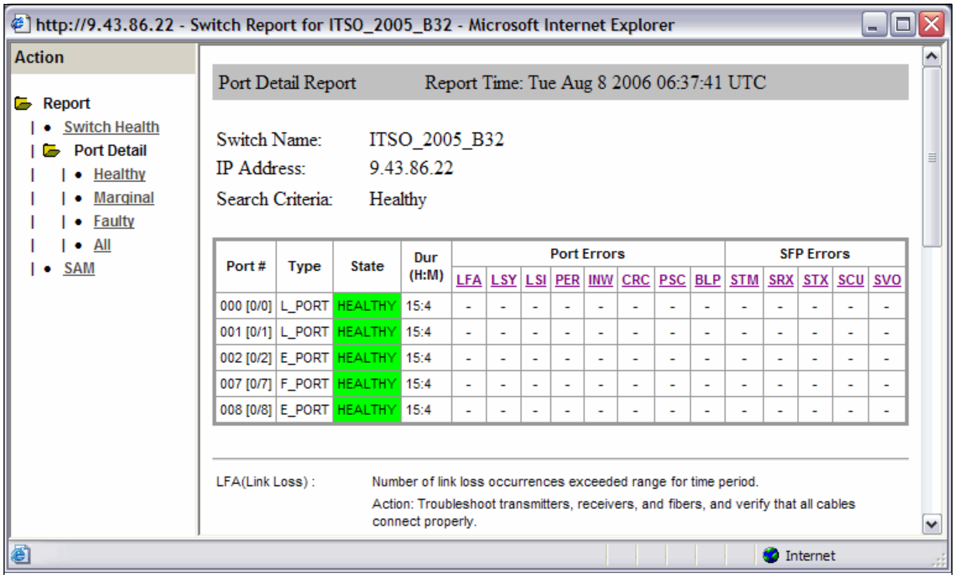
Switch Name: ITSO_2005_B32
IP Address: 9.43.86.22
Switch State: HEALTHY
Duration (H:M): 6: 16

Switch State Contributors	State
Power supplies monitor	HEALTHY
Temperatures monitor	HEALTHY
Fans monitor	HEALTHY
Flash monitor	HEALTHY
Marginal ports monitor	HEALTHY
Faulty ports monitor	HEALTHY
Missing SFPs monitor	HEALTHY

All ports are healthy.

Figure 1-63 SAN32B switch status view from WebTools

From here, we can navigate to obtain information about the health of the different ports on the switch. Under **Port Detail**, we can view the different ports in the *Healthy* status, *Marginal* status, and *Faulty* status. Clicking the **All** view displays details on all the ports. In Figure 1-64 we show the details for just the healthy ports. This information is helpful in understanding the port states.


http://9.43.86.22 - Switch Report for ITSO_2005_B32 - Microsoft Internet Explorer
Action
Report
Switch Health
Port Detail
Healthy
Marginal
Faulty
All
SAM
Internet

Port Detail Report Report Time: Tue Aug 8 2006 06:37:41 UTC

Switch Name: ITSO_2005_B32
IP Address: 9.43.86.22
Search Criteria: Healthy

Port #	Type	State	Dur (H:M)	Port Errors								SFP Errors				
				LFA	LSY	LSI	PER	INW	CRC	PSC	BLP	STM	SRX	STX	SCU	SVO
000 [0/0]	L_PORT	HEALTHY	15:4	-	-	-	-	-	-	-	-	-	-	-	-	-
001 [0/1]	L_PORT	HEALTHY	15:4	-	-	-	-	-	-	-	-	-	-	-	-	-
002 [0/2]	E_PORT	HEALTHY	15:4	-	-	-	-	-	-	-	-	-	-	-	-	-
007 [0/7]	F_PORT	HEALTHY	15:4	-	-	-	-	-	-	-	-	-	-	-	-	-
008 [0/8]	E_PORT	HEALTHY	15:4	-	-	-	-	-	-	-	-	-	-	-	-	-

LFA(Link Loss) : Number of link loss occurrences exceeded range for time period.
Action: Troubleshoot transmitters, receivers, and fibers, and verify that all cables connect properly.

```
- :  Monitoring value is within threshold.
X :  Monitoring value is over threshold.
```

Figure 1-64 SAN32B Port Detail Report

A full description of each of the columns is provided within the report view and is detailed in Table 1-12 for your reference.

Table 1-12 Port Detail Report - Error interpretation

Error	Description/ suggested action
LFA(Link Loss)	**Description:** Number of link loss occurrences exceeded range for time period.
	Action: Troubleshoot transmitters, receivers, and fibers, and verify that all cables connect properly.
LSY(Sync Loss)	**Description:** Number of sync loss occurrences exceeded range for time period.
	Action: Check for problems with the appropriate SFP and cable. If you continue to experience sync loss errors, troubleshoot your HBA and contact your support representative.
LSI(Signal Loss)	**Description:** Number of signal loss occurrences exceeded range for time period.
	Action: Troubleshoot transmitters, receivers, and fibers, and verify that all cables connect properly.
PER(Protocol Error)	**Description:** Number of protocol errors exceeded range for time period.
	Action: Check both ends of your connection, and verify that your cable and SFP are not faulty.
INW(Invalid Word)	**Description:** Number of invalid word exceeded range for time period.
	Action: Verify that your cable is not faulty and check both ends of your connection. Troubleshoot your SFP to verify that it is not faulty.
CRC(Invalid CRC)	**Description:** Number of invalid CRC errors exceeded range for time period.
	Action: Check your SFPs, cables, and connections for faulty hardware. Clean all optical hardware.
PSC(Port State)	**Description:** Port hardware state changed too often due to fabric reconfiguration.
	Action: All State Changes messages are informational. Respond to this message as is appropriate to the particular policy of the end-user installation.

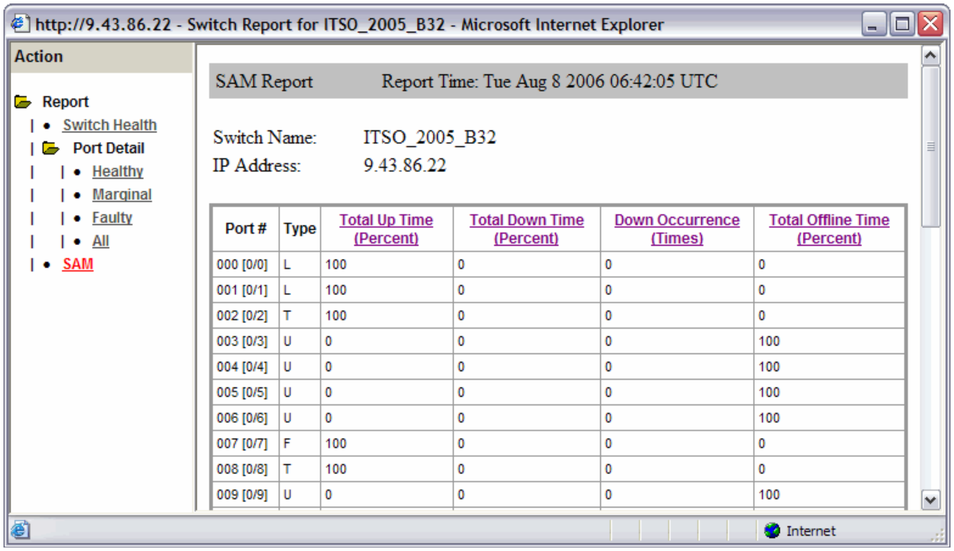
Error	Description/ suggested action
BLP(Buffer Limited Port)	**Description:** Port buffer credit was not large enough.
	Action: Reset the buffer credit.
STM(SFP Temperature)	**Description:** SFP temperature is out of specifications.
	Action: Temperature-related messages usually indicate that you must replace the SFP.
SRX(SFP RX)	**Description:** SFP receive power is out of specification.
	Action: Replace the SFP.
STX(SFP TX)	**Description:** SFP transmit power is out of specifications.
	Action: If the current rises above the high boundary, you must replace the SFP.
SCU(SFP Current)	**Description:** SFP current is out of specifications.
	Action: If the current rises above the high boundary, you must replace the SFP.
SVO(SFP Voltage)	**Description:** SFP voltage is out of specifications.
	Action: Frequent messages indicate that you must replace the SFP.

At a telnet prompt, the same information could be displayed by entering **`switchStatusShow`** command, as seen in Example 1-9.

Example 1-9 switchStatusShow output

```
ITSO_2005_B32:admin> switchStatusShow
Switch Health Report                            Report time: 08/10/2006 06:40:37 PM
Switch Name:    ITSO_2005_B32
IP address:     9.43.86.22
SwitchState:    HEALTHY
Duration:       27:10

Power supplies monitor  HEALTHY
Temperatures monitor    HEALTHY
Fans monitor            HEALTHY
Flash monitor           HEALTHY
Marginal ports monitor  HEALTHY
Faulty ports monitor    HEALTHY
Missing SFPs monitor    HEALTHY

All ports are healthy
```

Selecting SAM from the menu displays the Switch Availability Monitoring Report, as can be seen in Figure 1-65.


http://9.43.86.22 - Switch Report for ITSO_2005_B32 - Microsoft Internet Explorer
Action
Report
Switch Health
Port Detail
Healthy
Marginal
Faulty
All
SAM
Internet

SAM Report Report Time: Tue Aug 8 2006 06:42:05 UTC

Switch Name: ITSO_2005_B32
IP Address: 9.43.86.22

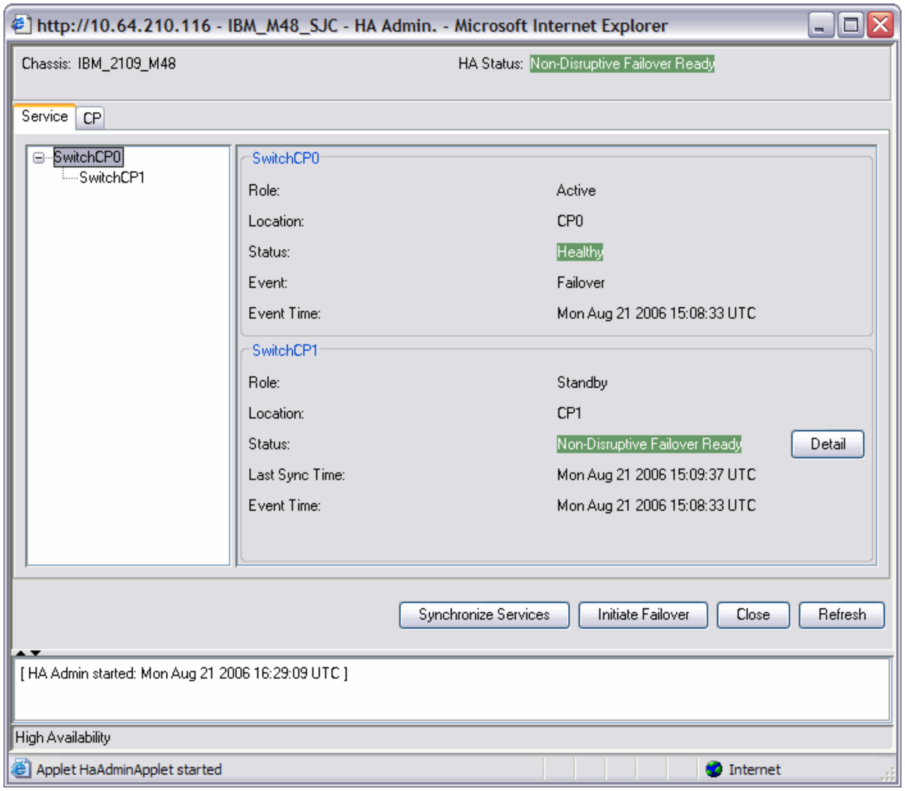
Port #	Type	Total Up Time (Percent)	Total Down Time (Percent)	Down Occurrence (Times)	Total Offline Time (Percent)
000 [0/0]	L	100	0	0	0
001 [0/1]	L	100	0	0	0
002 [0/2]	T	100	0	0	0
003 [0/3]	U	0	0	0	100
004 [0/4]	U	0	0	0	100
005 [0/5]	U	0	0	0	100
006 [0/6]	U	0	0	0	100
007 [0/7]	F	100	0	0	0
008 [0/8]	T	100	0	0	0
009 [0/9]	U	0	0	0	100

Figure 1-65 Switch Availability Monitoring Report

1.8.8 High Availability button

The M12, M14 and SAN256B are the only models with the High Availability features module. The background color of the **Hi Avail** button indicates the overall high availability status of the switch. It enables us to perform tasks such as CP failover or to synchronize services on the CP.

Clicking the **Hi Avail** button launches the High Availability services shown in Figure 1-66. The first tab shows the status of the Services for the switch. Notice that in the upper right corner the HA status field is green and displays: `Non-disruptive failover ready`. If the HA status field was other than green, then we would have to synchronize the services before attempting to initiate failover. When the HA status field shows `Non-disruptive failover ready`, a failover can be initiated without disrupting the fabric.


http://10.64.210.116 - IBM_M48_SJC - HA Admin. - Microsoft Internet Explorer
Service
CP
SwitchCP0
SwitchCP1
Detail
Synchronize Services
Initiate Failover
Close
Refresh
High Availability
Applet HaAdminApplet started
Internet

Chassis: IBM_2109_M48

HA Status: Non-Disruptive Failover Ready

SwitchCP0

Role: Active
Location: CP0
Status: Healthy
Event: Failover
Event Time: Mon Aug 21 2006 15:08:33 UTC

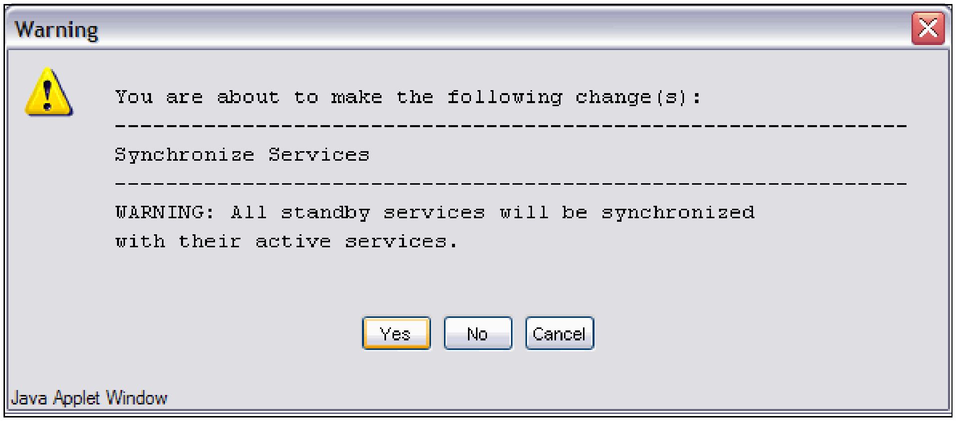
SwitchCP1

Role: Standby
Location: CP1
Status: Non-Disruptive Failover Ready
Last Sync Time: Mon Aug 21 2006 15:09:37 UTC
Event Time: Mon Aug 21 2006 15:08:33 UTC

```
[ HA Admin started: Mon Aug 21 2006 16:29:09 UTC ]
```

Figure 1-66 SAN 256B High availability Synchronize services

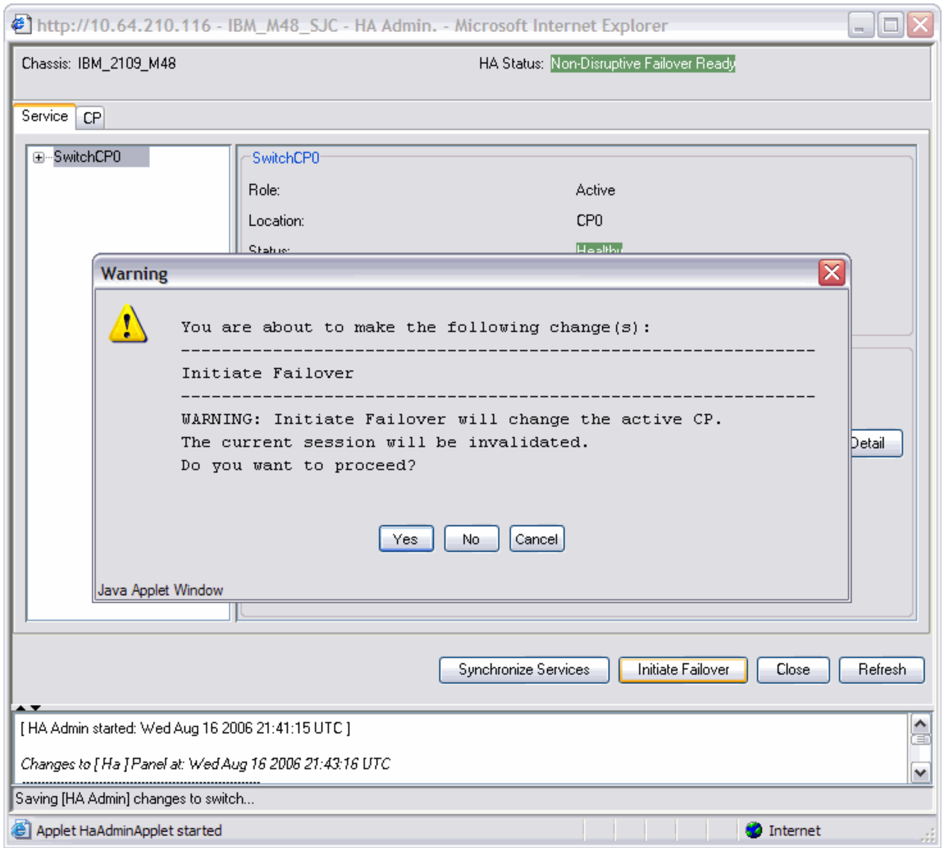
When selecting the **Synchronize Services** button, we are prompted with a warning asking us to confirm our actions as shown in Figure 1-67.



```
You are about to make the following change(s):
---------------------------------------------------------------
Synchronize Services
---------------------------------------------------------------
WARNING: All standby services will be synchronized
with their active services.
```

Figure 1-67 Warning synchronizing services

From the same panel we can initiate the failover and monitor the status as shown in Figure 1-68, by clicking the **Initiate Failover** button. Here we can see that CP0’s role is currently active.


http://10.64.210.116 - IBM_M48_SJC - HA Admin. - Microsoft Internet Explorer
Service
CP
SwitchCP0
SwitchCP0
Warning
Detail
Yes
No
Cancel
Java Applet Window
Synchronize Services
Initiate Failover
Close
Refresh
Applet HaAdminApplet started
Internet

Chassis: IBM_2109_M48

HA Status: Non-Disruptive Failover Ready

Role: Active

Location: CP0

Status:

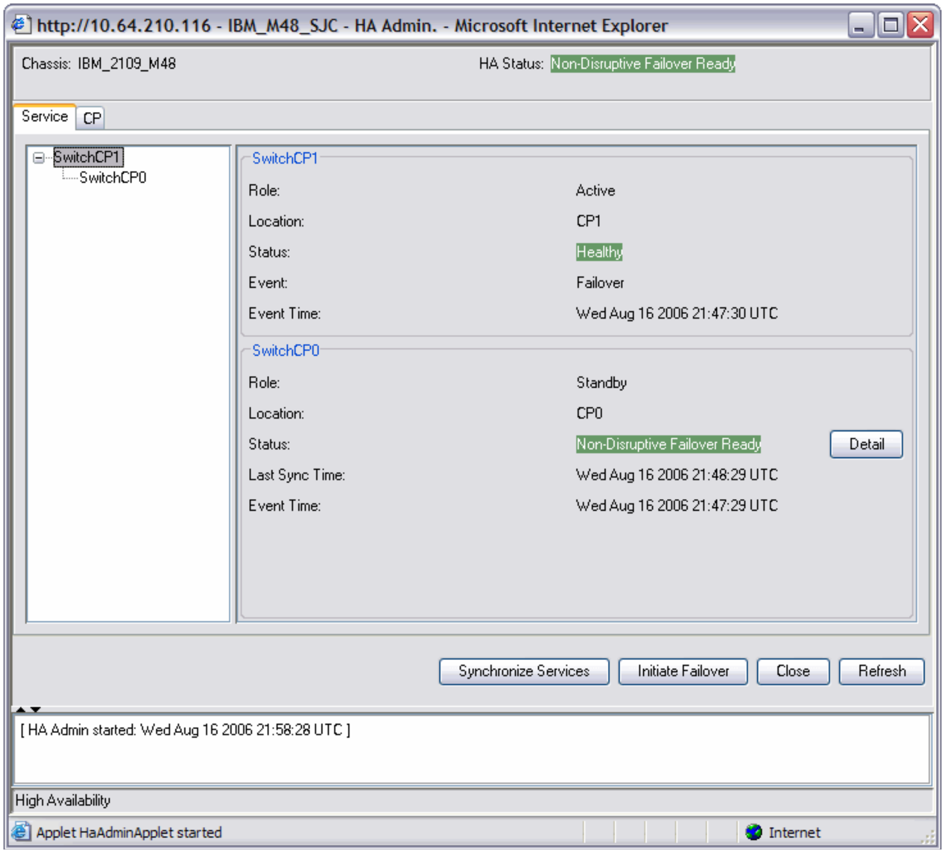
```
You are about to make the following change(s):
---------------------------------------------------------------
Initiate Failover
---------------------------------------------------------------
WARNING: Initiate Failover will change the active CP.
The current session will be invalidated.
Do you want to proceed?
```

```
[ HA Admin started: Wed Aug 16 2006 21:41:15 UTC ]

Changes to [ Ha ] Panel at: Wed Aug 16 2006 21:43:16 UTC
```

Saving [HA Admin] changes to switch...

Figure 1-68 SAN256B High Availability CP status

After clicking **Yes**, failover is initiated and the HA status field changes to red with the message, `Non-redundant failover` to indicate that failover is taking place. Just before it completes, HA status shows yellow and says `Disruptive Failover Ready`. When it has finally completed, we can see that the CPs have changed as shown in Figure 1-69 and HA status returns to `Non-Disruptive Failover Ready`.



http://10.64.210.116 - IBM_M48_SJC - HA Admin. - Microsoft Internet Explorer

Chassis: IBM_2109_M48

HA Status: Non-Disruptive Failover Ready

SwitchCP1

Role: Active

Location: CP1

Status: Healthy

Event: Failover

Event Time: Wed Aug 16 2006 21:47:30 UTC

SwitchCP0

Role: Standby

Location: CP0

Status: Non-Disruptive Failover Ready

Last Sync Time: Wed Aug 16 2006 21:48:29 UTC

Event Time: Wed Aug 16 2006 21:47:29 UTC

[HA Admin started: Wed Aug 16 2006 21:58:28 UTC]

Applet HaAdminApplet started

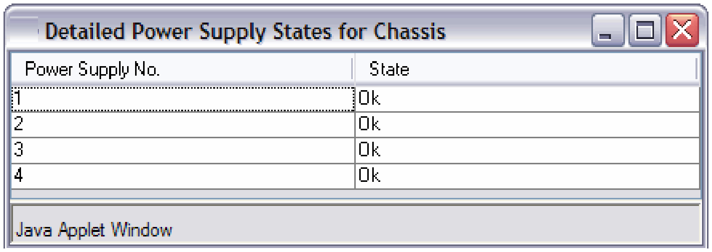
Service
CP
SwitchCP1
SwitchCP0
Detail
Synchronize Services
Initiate Failover
Close
Refresh
High Availability
Internet

Figure 1-69 SAN256B failover complete

> **Note:** A non-disruptive failover might take a few minutes to complete, and it is possible that the connection to the switch might be lost during that time.

1.8.9 Power button

The background color of the **Power** button indicates the overall health of the power supply status. Clicking **Power** displays the window shown in Figure 1-70.


Detailed Power Supply States for Chassis

Power Supply No.	State
1	Ok
2	Ok
3	Ok
4	Ok

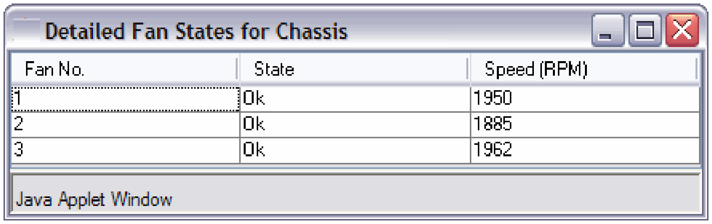
Java Applet Window

Figure 1-70   SAN256B power status

1.8.10 Fan button

The **Fan button** is an alerting icon on all models except the SAN256B. If all conditions are normal according to the switch policy settings, the icon should be green. On the SAN256B, it is a chassis wide status button.

Clicking the **Fan** button displays an informational window describing the state of each fan, as shown in Figure 1-71.


Detailed Fan States for Chassis

Fan No.	State	Speed (RPM)
1	Ok	1950
2	Ok	1885
3	Ok	1962

Java Applet Window

Figure 1-71   SAN256B Fan Status

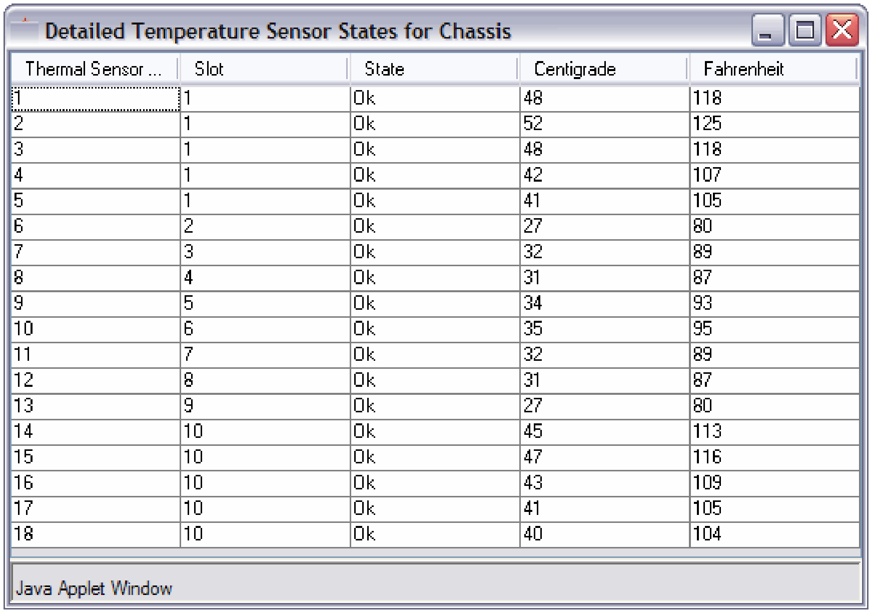
It is possible to gather the same information from a telnet command line by typing **`fanshow`** as shown in Example 1-10.

Example 1-10   M48 fanshow CLI command

```
IBM_M48_SJC:admin> fanShow
Fan 1 is Ok, speed is 1950 RPM
Fan 2 is Ok, speed is 1885 RPM
Fan 3 is Ok, speed is 1973 RPM
```

1.8.11 Temp button

The **Temp button** is an alerting icon on all switch models except the SAN256B. It changes color, from green to show that all temperatures are within the defined limits, to yellow or red depending on the policy thresholds. On the SAN256B, clicking the **Temp** button displays detailed temperature information for the chassis shown in Figure 1-72.



Detailed Temperature Sensor States for Chassis

Thermal Sensor ...	Slot	State	Centigrade	Fahrenheit
1	1	Ok	48	118
2	1	Ok	52	125
3	1	Ok	48	118
4	1	Ok	42	107
5	1	Ok	41	105
6	2	Ok	27	80
7	3	Ok	32	89
8	4	Ok	31	87
9	5	Ok	34	93
10	6	Ok	35	95
11	7	Ok	32	89
12	8	Ok	31	87
13	9	Ok	27	80
14	10	Ok	45	113
15	10	Ok	47	116
16	10	Ok	43	109
17	10	Ok	41	105
18	10	Ok	40	104

Java Applet Window

Figure 1-72 SAN256B Temperature status window

To display similar information at a telnet command line, issue the **`tempShow`** command as shown in Example 1-11.

Example 1-11 SAN256B tempShow output

```
IBM_M48_SJC:admin> tempShow
Sensor  Slot    State   Centigrade     Fahrenheit
  ID
=====================================================
  1      1      Ok          48            118
  2      1      Ok          52            125
  3      1      Ok          48            118
  4      1      Ok          42            107
  5      1      Ok          41            105
  6      2      Ok          27             80
  7      3      Ok          32             89
  8      4      Ok          31             87
  9      5      Ok          34             93
 10      6      Ok          35             95
 11      7      Ok          32             89
 12      8      Ok          31             87
 13      9      Ok          27             80
 14     10      Ok          45            113
 15     10      Ok          47            116
 16     10      Ok          43            109
 17     10      Ok          41            105
 18     10      Ok          40            104
```

1.8.12 Admin button

Previously, we showed how to configure many settings using the Command Line Interface. Most of these settings can also be configured using the WebTools Administration Tools interface.

To perform administration and setup functions on a single switch, we select the appropriate switch from the fabric view. Then, from the switch view frame, we click the **Admin** button as shown in Figure 1-73.

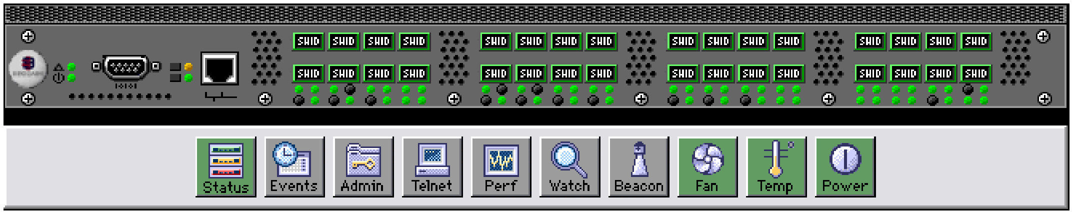
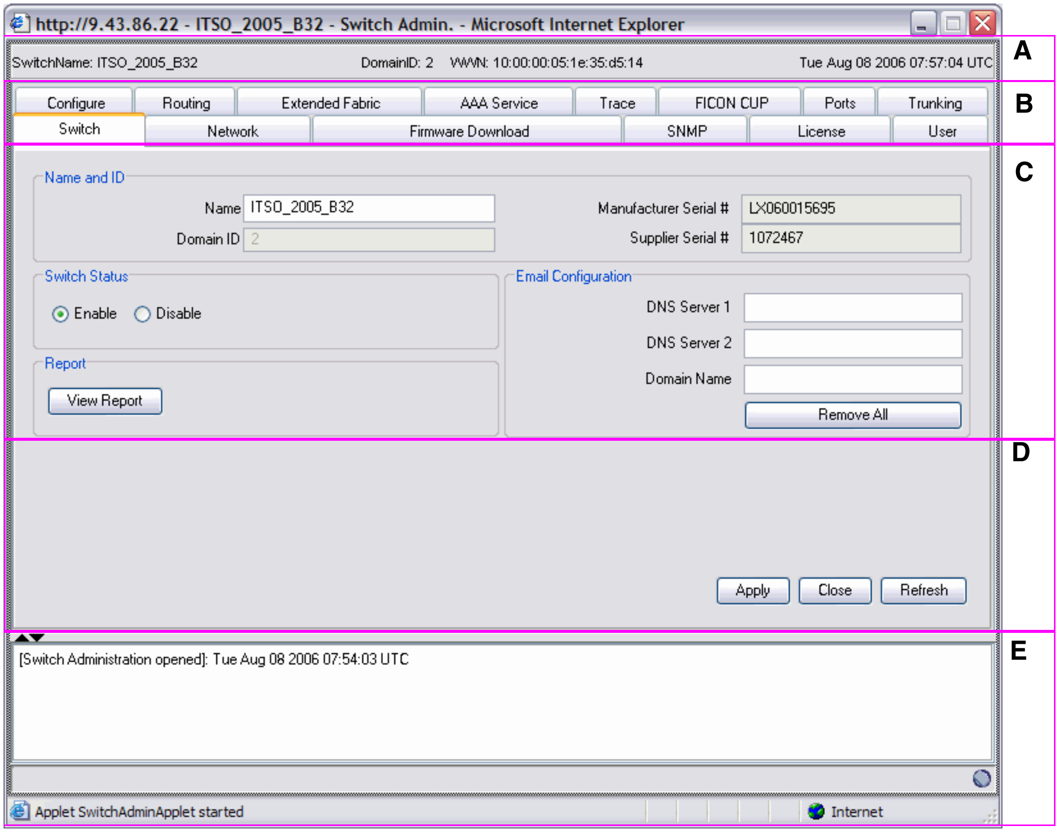


Figure 1-73 SAN32B Admin tools from WebTools

Administration tools window layout

When the administration window has opened, we can see that it is composed of five areas (labeled A, B, C, D, E) as shown in Figure 1-74.

> **Tip:** By hovering the mouse over buttons and other *areas* of the window, you can find out their function.



http://9.43.86.22 - ITSO_2005_B32 - Switch Admin. - Microsoft Internet Explorer

SwitchName: ITSO_2005_B32 DomainID: 2 WWN: 10:00:00:05:1e:35:d5:14 Tue Aug 08 2006 07:57:04 UTC

Name and ID

Name: ITSO_2005_B32

Domain ID: 2

Manufacturer Serial #: LX060015695

Supplier Serial #: 1072467

Switch Status

● Enable ○ Disable

Email Configuration

DNS Server 1:

DNS Server 2:

Domain Name:

[Switch Administration opened]: Tue Aug 08 2006 07:54:03 UTC

Applet SwitchAdminApplet started

A
B
C
D
E
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Ports
Trunking
Switch
Network
Firmware Download
SNMP
License
User
Report
View Report
Remove All
Apply
Close
Refresh
Internet

Figure 1-74 SAN-32B Administration window layout

- **Area A:** Displays summary information, switch name, domain ID, date, time.
- **Area B:** Allows navigation through the different management panels. The content of this area depends on the licenses installed on the switch.
- **Area C:** Contains parameters to be set in the current panel.
- **Area D:** Contains the button bar.
- **Area E:** Contains the report window that allows viewing of the switch report upon operation completion.

Switch Information

When the administration window is first opened, the **Switch Information** tab is then displayed by default, as shown in Figure 1-74.

On the first tab we can define the switch name and the domain ID, set the base e-mail configuration, enable or disable the entire switch, and view a detailed report of the switch.

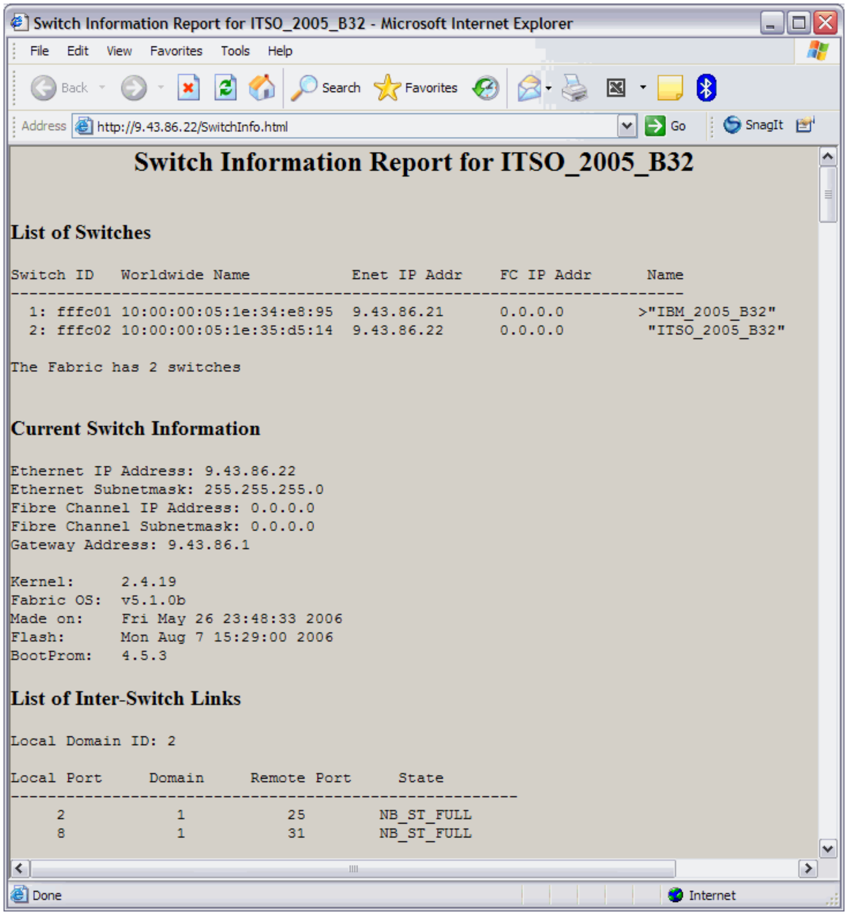
Table 1-13 describes the fields on the **Switch Information** tab.

Table 1-13 Switch Information tab

Field	Description
Name	Enter data for the switch name. Enter a new name to change a name in this field.
Domain ID	Displays or sets switch domain ID. Domain IDs must be unique within a fabric. To change domain ID, enter new domain ID in this field. Use a number from 1 to 239 for normal operating mode (FCSW compatible) and a number from 0 to 31 for VC encoded address format mode (backward compatible to SilkWorm 1000 series).
Manufacturer Serial #	Physical serial number of the switch.
Supplier Serial #	Supplier serial number of switch for display only.
(Status) Enable	Click the radio button to enable the switch.
(Status) Disable	Click the radio button to disable the switch.
Apply	Click to save any changes made to this tab and remain in the current tab. Additional changes can be made and the **Apply** button clicked when making changes incrementally.
Close	Click to exit the Switch Admin view. If changes have been made and not committed by clicking the **Apply** button, a dialog box is presented. It allows the changes to be committed or deleted.
Reset	Click to reset the tab to the last set of saved changes.
Refresh	Click to retrieve current values from the switch.

View Report

Clicking the **View Report** button displays a window as shown in Figure 1-75. The detailed report includes a list of all the types of switches connected to our local switch, the inter-switch links, list of ports, the Name Server information, details on the configured zones, and SFP serial ID information.


Switch Information Report for ITSO_2005_B32 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://9.43.86.22/SwitchInfo.html
Go
SnagIt
Done
Internet

Switch Information Report for ITSO_2005_B32

List of Switches

```
Switch ID   Worldwide Name           Enet IP Addr    FC IP Addr      Name
-------------------------------------------------------------------------
  1: fffc01 10:00:00:05:1e:34:e8:95  9.43.86.21      0.0.0.0        >"IBM_2005_B32"
  2: fffc02 10:00:00:05:1e:35:d5:14  9.43.86.22      0.0.0.0         "ITSO_2005_B32"

The Fabric has 2 switches
```

Current Switch Information

```
Ethernet IP Address: 9.43.86.22
Ethernet Subnetmask: 255.255.255.0
Fibre Channel IP Address: 0.0.0.0
Fibre Channel Subnetmask: 0.0.0.0
Gateway Address: 9.43.86.1

Kernel:     2.4.19
Fabric OS:  v5.1.0b
Made on:    Fri May 26 23:48:33 2006
Flash:      Mon Aug 7 15:29:00 2006
BootProm:   4.5.3
```

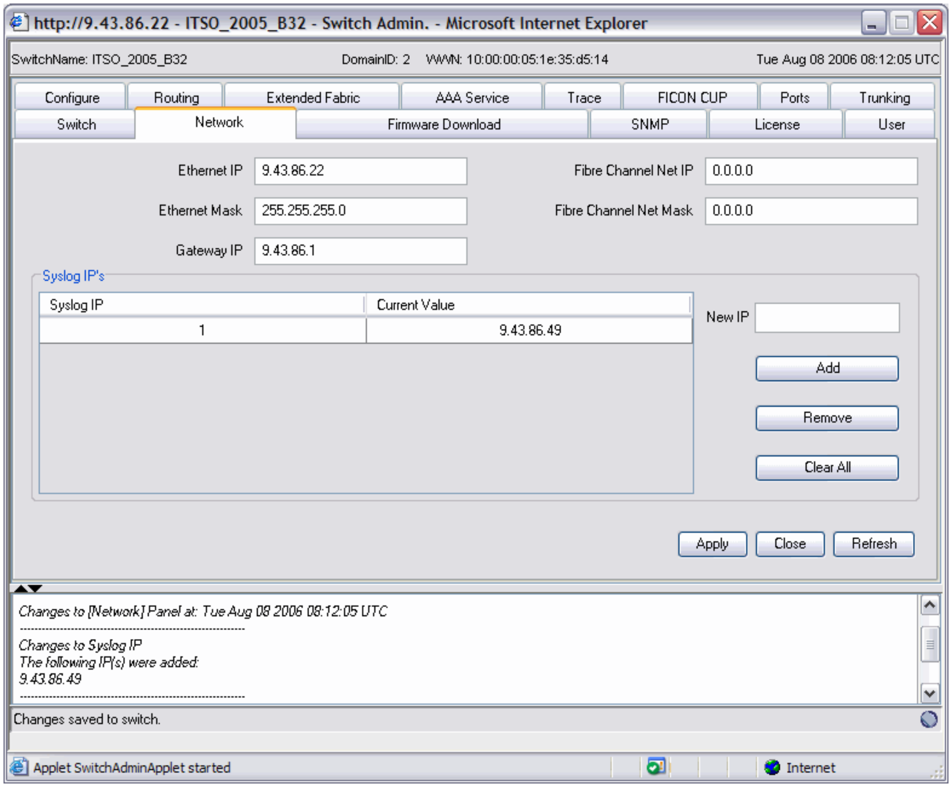
List of Inter-Switch Links

```
Local Domain ID: 2

Local Port     Domain     Remote Port     State
-------------------------------------------------------
     2            1           25        NB_ST_FULL
     8            1           31        NB_ST_FULL
```

Figure 1-75 SAN32B Switch report

Network Config tab

Use the **Network Config** tab to modify the IP settings of the switch as shown in Figure 1-76.


http://9.43.86.22 - ITSO_2005_B32 - Switch Admin. - Microsoft Internet Explorer
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Ports
Trunking
Switch
Network
Firmware Download
SNMP
License
User
Syslog IP's
New IP
Add
Remove
Clear All
Apply
Close
Refresh
Internet

SwitchName: ITSO_2005_B32 DomainID: 2 WWN: 10:00:00:05:1e:35:d5:14 Tue Aug 08 2006 08:12:05 UTC

Ethernet IP 9.43.86.22

Ethernet Mask 255.255.255.0

Gateway IP 9.43.86.1

Fibre Channel Net IP 0.0.0.0

Fibre Channel Net Mask 0.0.0.0

Syslog IP	Current Value
1	9.43.86.49

```
Changes to [Network] Panel at: Tue Aug 08 2006 08:12:05 UTC
----------------------------------------------------------------
Changes to Syslog IP
The following IP(s) were added:
9.43.86.49
----------------------------------------------------------------
```

Changes saved to switch.

Applet SwitchAdminApplet started

Figure 1-76 SAN32B Network Config panel

Table 1-14 describes the fields on the **Network Config** tab.

Table 1-14 Network Config tab

Field	Description
Ethernet IP	Display or set the Ethernet IP address
Ethernet Mask	Display or set the Ethernet IP Subnet Mask.
Gateway IP	Display or set the Gateway IP address.
Fibre Channel Net IP	Display or set the Fibre Channel IP address.
Fibre Channel Net Mask	Display the Fibre Channel SubnetMask address.
Syslog IPs	Display the six syslog IP addresses for a user to configure.
Add	Add syslog IP address entered in field.
Remove	Remove syslog IP address in field.
Clear All	Remove all previous syslog IP entries.
Apply	Click to save the changes made to this tab and to stay in the current tab. Additional changes can be made and the **Apply** button can be clicked when making changes incrementally.
Close	Click to exit the Admin window. If changes have been made but not committed by clicking the **Apply** button, a dialog box displays.
Refresh	Click to retrieve current values from the switch.

Overview of syslogd

The Fabric OS maintains an internal log of all error messages, but the internal log buffers are limited in capacity; when the internal buffers are full, new messages overwrite old messages.

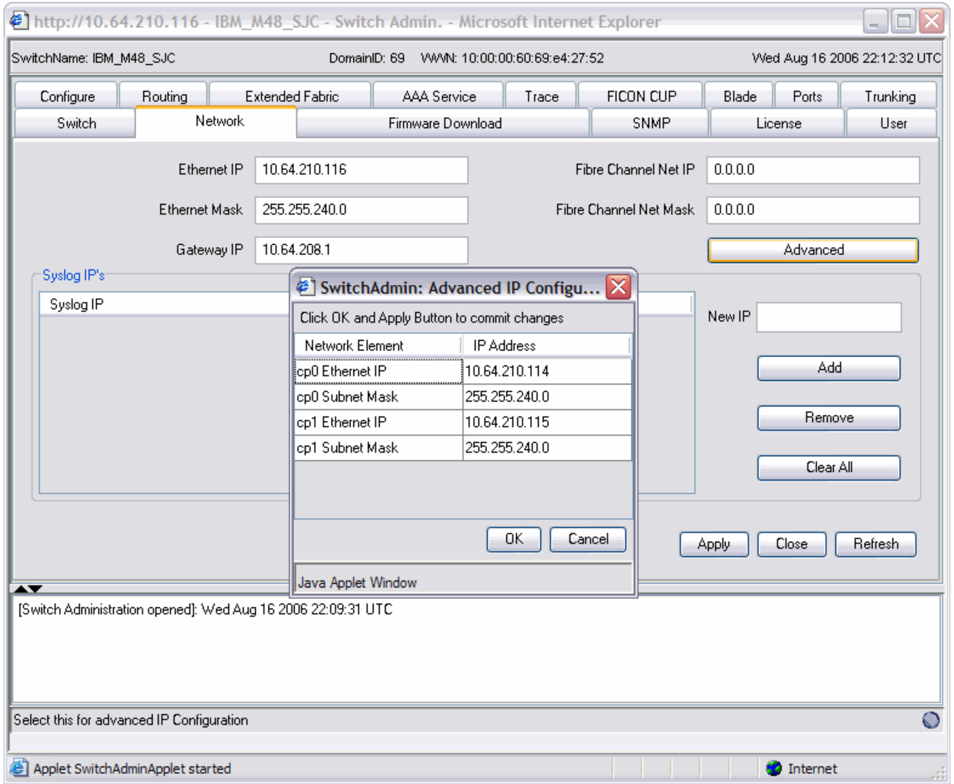
The IBM TotalStorage SAN Switch can be configured to send error log messages to a UNIX host system that supports `syslogd`. This host system can be configured to receive error/event messages from the switch and store them in its file system, overcoming the size limitations of the internal log buffers on the switch.

The host system can be running UNIX, Linux, or any other operating system as long as it supports standard `syslogd` functionality. The IBM TotalStorage SAN Switch by itself does not assume any particular operating system to be running on the host system.

To configure the syslog function, we simply put the IP address of the host running the `syslogd` in the **Syslog IP** field, and click **Add**. After adding all logging host IP addresses to the list, we must click **Apply** to save the changes.

Network Config

When configuring the network settings on a director using this tab, extra care should be taken that we have opened the Admin function for the correct logical switch, as the settings only apply to that logical switch. The **`Advanced`** button can be selected in order to set the IP address and subnet mask for each CP, as shown in Figure 1-77.



Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Blade
Ports
Trunking
Switch
Network
Firmware Download
SNMP
License
User
Advanced
Syslog IP's
Syslog IP
New IP
Add
Remove
Clear All
OK
Cancel
Apply
Close
Refresh
Internet

http://10.64.210.116 - IBM_M48_SJC - Switch Admin. - Microsoft Internet Explorer

SwitchName: IBM_M48_SJC DomainID: 69 WWN: 10:00:00:60:69:e4:27:52 Wed Aug 16 2006 22:12:32 UTC

Ethernet IP: 10.64.210.116
Ethernet Mask: 255.255.240.0
Gateway IP: 10.64.208.1
Fibre Channel Net IP: 0.0.0.0
Fibre Channel Net Mask: 0.0.0.0

SwitchAdmin: Advanced IP Configu...

Click OK and Apply Button to commit changes

Network Element	IP Address
cp0 Ethernet IP	10.64.210.114
cp0 Subnet Mask	255.255.240.0
cp1 Ethernet IP	10.64.210.115
cp1 Subnet Mask	255.255.240.0

Java Applet Window

[Switch Administration opened]: Wed Aug 16 2006 22:09:31 UTC

Select this for advanced IP Configuration

Applet SwitchAdminApplet started

Figure 1-77 Admin View - Network config of the SAN256B

These same settings were configured earlier by using the command line install procedure, detailed in the “SAN256B configuration procedure” on page 49.

Firmware tab

We use the Firmware tab to perform the following actions:

- Download firmware
- Reboot switch
- Fastboot switch

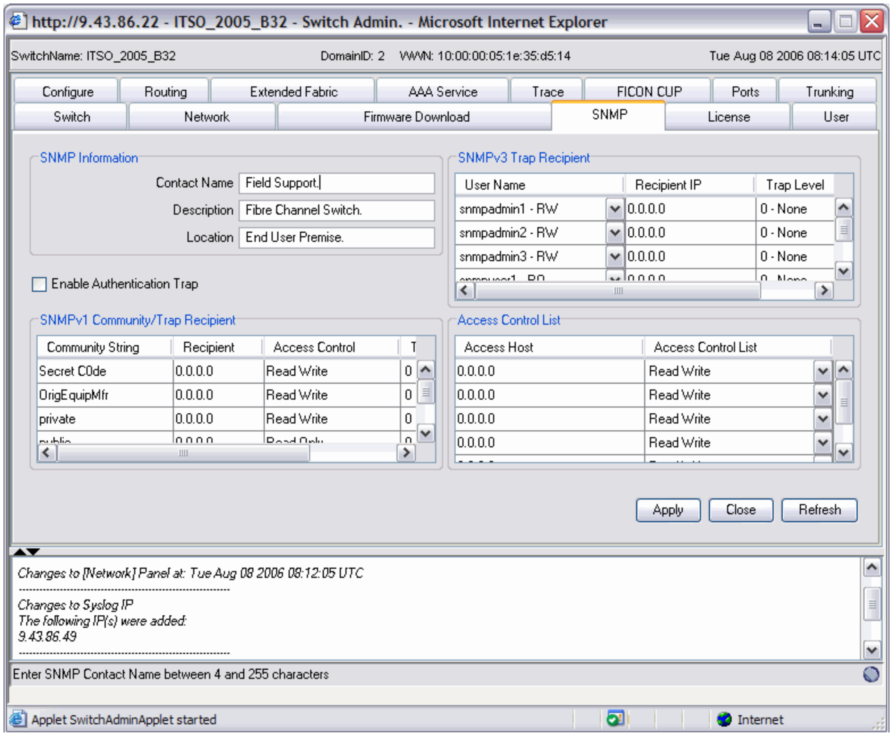
We always recommend that you upload a copy of the switch configuration before performing any firmware change. These configuration upload functions have been moved to the **Configure** tab under “Configure tab” on page 141.

For full details of how to download new firmware via WebTools, refer to “Upgrading the firmware using the WebTools” on page 272.

SNMP tab

Use the SNMP tab for administration of the SNMP Subsystem. From the SNMP tab, we can specify the switch community string, location, trap level, and trap recipients. SNMP v3 is available from FOS 4.4 onwards, as well as SNMP v1. As shown in Figure 1-78, traps can be set using either SNMP v1 or SNMP v3.

SNMP parameters can also be set with Telnet commands or Fabric Manager.


http://9.43.86.22 - ITSO_2005_B32 - Switch Admin. - Microsoft Internet Explorer
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Ports
Trunking
Switch
Network
Firmware Download
SNMP
License
User
Apply
Close
Refresh
Applet SwitchAdminApplet started
Internet

SwitchName: ITSO_2005_B32 DomainID: 2 WWN: 10:00:00:05:1e:35:d5:14 Tue Aug 08 2006 08:14:05 UTC

SNMP Information

Contact Name: Field Support.

Description: Fibre Channel Switch.

Location: End User Premise.

☐ Enable Authentication Trap

SNMPv3 Trap Recipient

User Name	Recipient IP	Trap Level
snmpadmin1 - RW	0.0.0.0	0 - None
snmpadmin2 - RW	0.0.0.0	0 - None
snmpadmin3 - RW	0.0.0.0	0 - None

SNMPv1 Community/Trap Recipient

Community String	Recipient	Access Control	T
Secret C0de	0.0.0.0	Read Write	0
OrigEquipMfr	0.0.0.0	Read Write	0
private	0.0.0.0	Read Write	0

Access Control List

Access Host	Access Control List
0.0.0.0	Read Write
0.0.0.0	Read Write
0.0.0.0	Read Write
0.0.0.0	Read Write

```
Changes to [Network] Panel at: Tue Aug 08 2006 08:12:05 UTC
------------------------------------------------------------
Changes to Syslog IP
The following IP(s) were added:
9.43.86.49
------------------------------------------------------------
```

Enter SNMP Contact Name between 4 and 255 characters

Figure 1-78 SNMP tab

To create a new SNMPv1 trap

Create a new trap as follows:

1. Double-click a community string in the SNMPv1 section and type a new community string.
2. Double-click a recipient IP address in the SNMPv1 section and type a new IP address.
3. Click **Apply**.

To create a new SNMPv3 trap

Create a new trap as follows:

1. Select a user name from the User Name drop-down list in the SNMPv3 section.
2. Double-click a recipient IP address in the SNMP v3 section and type a new IP address.
3. Select a trap level from the Trap Level drop-down list.
4. Click **Apply**.

In Table 1-15 we describe the fields on the **SNMP** tab.

Table 1-15 SNMP tab

SNMP Basic information:	
Contact Name	Displays or sets contact information for switch. Default is Field Support.
Description	Displays or sets system description. Default is Fibre Channel Switch.
Location	Displays or sets the location of switch. Default is End User Premise.
Enable Authentication Trap	Check to enable authentication traps; uncheck to disable (recommended).
SNMPv1 Community/Trap Recipient:	
Community String	Displays the community strings that are available to use. A community refers to a relationship between a group of SNMP managers and an SNMP agent, in which authentication, access control, and proxy characteristics are defined. A maximum of six community strings can be saved to the switch.
Recipient	Displays the IP address of the Trap Recipient. A trap recipient receives the message sent by an SNMP agent to inform the SNMP management station of a critical error.

Access Control	Displays the Read/Write access of a particular community string. Read only access means that a member of a community string has the right to view, but cannot be changed. Read/Write access means that a member of a community string can be both viewed and changed.
Trap Level	Sets severity level of switch events that prompt SNMP traps. Default is 0.
SNMPv3 Trap Recipient:	
User Name	Displays user names that are available to use. The user names are predefined with different Read/Write or Read Only access. The predefined user names are snmpadmin1, snmpadmin2, snmpadmin3 with Read/Write access and snmpuser1, snmpuser2, snmpuser3 with Read Only access.
Recipient IP	Displays the IP address of the Trap Recipient. A trap recipient receives the message sent by an SNMP agent to inform the SNMP management station of a critical error.
Trap Level	Sets severity level of switch events that prompt SNMP traps. Default is 0
Access Control List Configuration:	
Access Host	Displays the IP address of the host of the access list.
Access Control List	Displays the Read/Write access of a particular access list. Read only access means that a member of an access list has the right to view, but cannot make changes. Read/Write access means that a member of an access list can both view and make changes.
Apply	Click to save the changes made to this tab. Additional changes can be made and the **Apply** button clicked when making changes incrementally.
Close	Click to exit the Admin Window. If changes have been made but not committed by clicking the **Apply** button, a dialog box displays.
Refresh	Click to retrieve current values from the switch.

We can also set SNMP parameters with Telnet using the **`agtcfgSet`** command and the **`agtcfgShow`** command to display the current SNMP settings. To reset the default settings we use the command **`agtcfgDefault`**.

> **Note:** In order for the switches to send SNMP traps, we must first enter the Telnet command **`snmpMibCapSet`**. This enables the MIBs on all switches to be monitored.

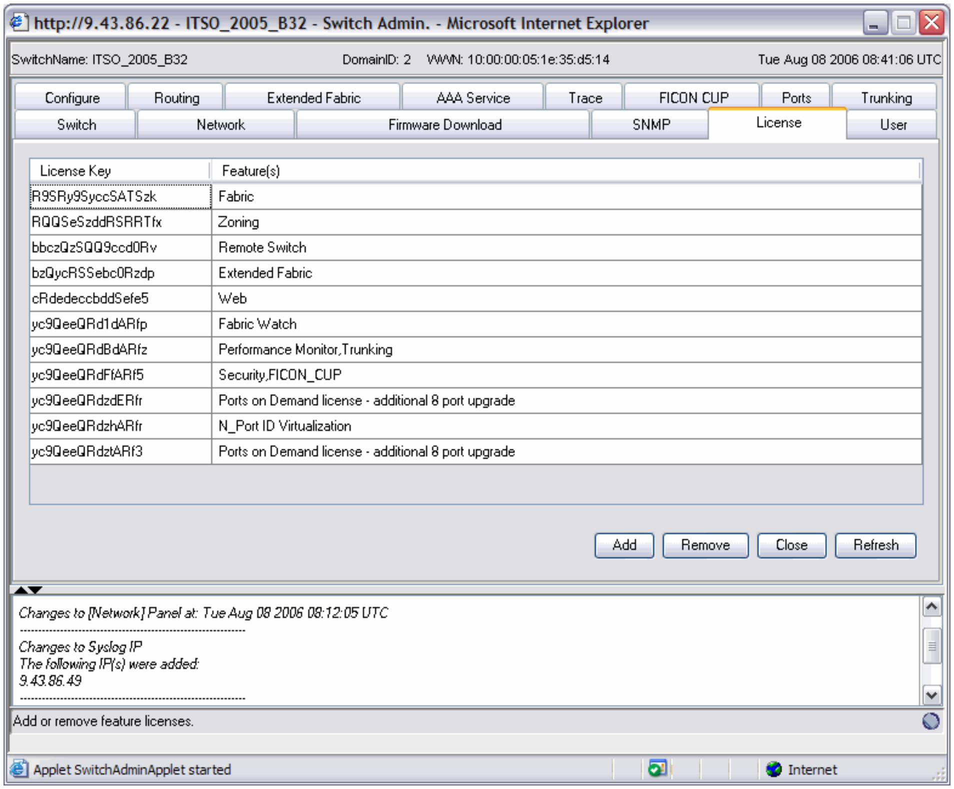
Example 1-12 details the output from the **`snmpMibCapSet`** command.

Example 1-12 CLI output from snmpMibCapSet

```
ITSO_2005_B32:admin> snmpMibCapSet
The SNMP Mib/Trap Capability has been set to support
FE-MIB
SW-MIB
FA-MIB
FICON-MIB
HA-MIB
SW-TRAP
   swFCPortScn
   swEventTrap
   swFabricWatchTrap
   swTrackChangesTrap
FA-TRAP
   connUnitStatusChange
   connUnitEventTrap
   connUnitSensorStatusChange
   connUnitPortStatusChange
FICON-TRAP
   linkRNIDDeviceRegistration
   linkRNIDDeviceDeRegistration
  linkLIRRListenerAdded
   linkLIRRListenerRemoved
   linkRLIRFailureIncident
HA-TRAP
   fruStatusChanged
   cpStatusChanged
   fruHistoryTrap
FA-MIB (yes, y, no, n): [yes]
```

License tab

We use the **License** tab to install the license keys that have been purchased. License keys are used to enable additional features on a switch. We can also use the table within the **License** tab to remove a listed license from the switch. The **License** tab is shown in Figure 1-79.


http://9.43.86.22 - ITSO_2005_B32 - Switch Admin. - Microsoft Internet Explorer
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Ports
Trunking
Switch
Network
Firmware Download
SNMP
License
User
Add
Remove
Close
Refresh
Applet SwitchAdminApplet started
Internet

SwitchName: ITSO_2005_B32 DomainID: 2 WWN: 10:00:00:05:1e:35:d5:14 Tue Aug 08 2006 08:41:06 UTC

License Key	Feature(s)
R9SRy9SyccSATSzk	Fabric
RQQSeSzddRSRRTfx	Zoning
bbczQzSQQ9ccd0Rv	Remote Switch
bzQycRSSebc0Rzdp	Extended Fabric
cRdedeccbddSefe5	Web
yc9QeeQRd1dARfp	Fabric Watch
yc9QeeQRdBdARfz	Performance Monitor,Trunking
yc9QeeQRdFfARf5	Security,FICON_CUP
yc9QeeQRdzdERfr	Ports on Demand license - additional 8 port upgrade
yc9QeeQRdzhARfr	N_Port ID Virtualization
yc9QeeQRdztARf3	Ports on Demand license - additional 8 port upgrade

```
Changes to [Network] Panel at: Tue Aug 08 2006 08:12:05 UTC
------------------------------------------------------------
Changes to Syslog IP
The following IP(s) were added:
9.43.86.49
------------------------------------------------------------
```

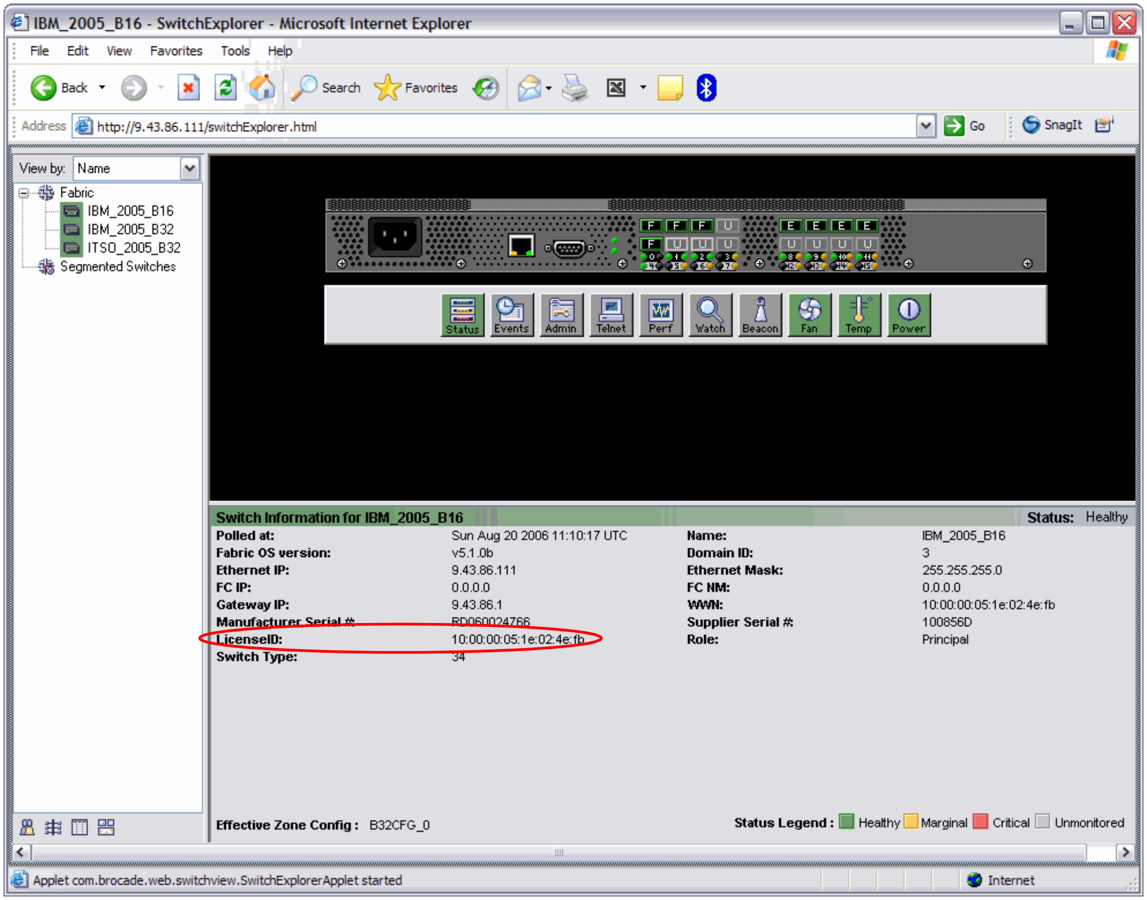
Add or remove feature licenses.

Figure 1-79 Installed License keys

Before we can enable any additional feature licenses purchased, we must first acquire the feature activation key.

We start by obtaining the license ID of the switch using either the GUI or CLI as detailed:

- **GUI:** Start the Web browser if is not already active. Enter the switch IP address. The license ID of the switch displays on the Switch Information panel. Figure 1-80 highlights the LicenseID on the browser page.


IBM_2005_B16 - SwitchExplorer - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://9.43.86.111/switchExplorer.html
Go
SnagIt
View by: Name
Fabric
IBM_2005_B16
IBM_2005_B32
ITSO_2005_B32
Segmented Switches
Status
Events
Admin
Telnet
Perf
Watch
Beacon
Fan
Temp
Power
Applet com.brocade.web.switchview.SwitchExplorerApplet started
Internet

Switch Information for IBM_2005_B16 Status: Healthy

Polled at: Sun Aug 20 2006 11:10:17 UTC
Fabric OS version: v5.1.0b
Ethernet IP: 9.43.86.111
FC IP: 0.0.0.0
Gateway IP: 9.43.86.1
Manufacturer Serial #: RD060024766
LicenseID: 10:00:00:05:1e:02:4e:fb
Switch Type: 34
Name: IBM_2005_B16
Domain ID: 3
Ethernet Mask: 255.255.255.0
FC NM: 0.0.0.0
WWN: 10:00:00:05:1e:02:4e:fb
Supplier Serial #: 100856D
Role: Principal

Effective Zone Config : B32CFG_0

Status Legend : 🟩 Healthy 🟨 Marginal 🟥 Critical ☐ Unmonitored

Figure 1-80 Viewing the switch LicenseID

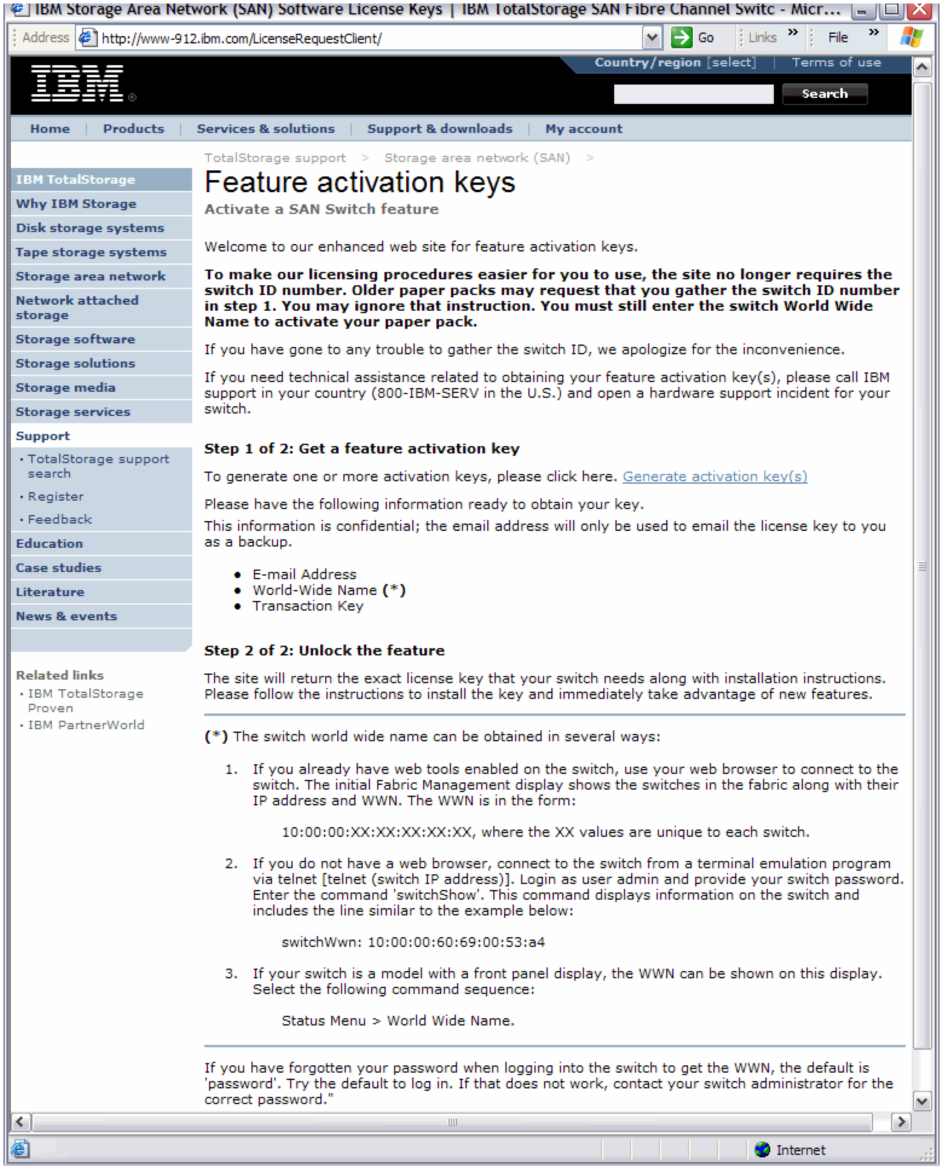
- **CLI:** Telnet to the switch via its IP address and log in as admin. Enter the **`licenseidshow`** command to display the license ID of the switch.

  The WWN is in the form 10:00:xx:xx:xx:xx:xx:xx, where xx values are unique to each switch.

Next we enter the following Address in our Web browser:

`http://www.ibm.com/storage/key`

The Web page presented in Figure 1-81 details the process for generating the Feature activation keys.


IBM Storage Area Network (SAN) Software License Keys | IBM TotalStorage SAN Fibre Channel Switc - Micr...
Address http://www-912.ibm.com/LicenseRequestClient/
Go
Links
File
IBM
Country/region [select]
Terms of use
Search
Home
Products
Services & solutions
Support & downloads
My account
IBM TotalStorage
Why IBM Storage
Disk storage systems
Tape storage systems
Storage area network
Network attached storage
Storage software
Storage solutions
Storage media
Storage services
Support
· TotalStorage support search
· Register
· Feedback
Education
Case studies
Literature
News & events
Related links
· IBM TotalStorage Proven
· IBM PartnerWorld
TotalStorage support > Storage area network (SAN) >
Internet

Feature activation keys

Activate a SAN Switch feature

Welcome to our enhanced web site for feature activation keys.

To make our licensing procedures easier for you to use, the site no longer requires the switch ID number. Older paper packs may request that you gather the switch ID number in step 1. You may ignore that instruction. You must still enter the switch World Wide Name to activate your paper pack.

If you have gone to any trouble to gather the switch ID, we apologize for the inconvenience.

If you need technical assistance related to obtaining your feature activation key(s), please call IBM support in your country (800-IBM-SERV in the U.S.) and open a hardware support incident for your switch.

Step 1 of 2: Get a feature activation key

To generate one or more activation keys, please click here. Generate activation key(s)

Please have the following information ready to obtain your key.

This information is confidential; the email address will only be used to email the license key to you as a backup.

- E-mail Address
- World-Wide Name **(*)**
- Transaction Key

Step 2 of 2: Unlock the feature

The site will return the exact license key that your switch needs along with installation instructions. Please follow the instructions to install the key and immediately take advantage of new features.

(*) The switch world wide name can be obtained in several ways:

1. If you already have web tools enabled on the switch, use your web browser to connect to the switch. The initial Fabric Management display shows the switches in the fabric along with their IP address and WWN. The WWN is in the form:

   10:00:00:XX:XX:XX:XX:XX, where the XX values are unique to each switch.

2. If you do not have a web browser, connect to the switch from a terminal emulation program via telnet [telnet (switch IP address)]. Login as user admin and provide your switch password. Enter the command 'switchShow'. This command displays information on the switch and includes the line similar to the example below:

   switchWwn: 10:00:00:60:69:00:53:a4

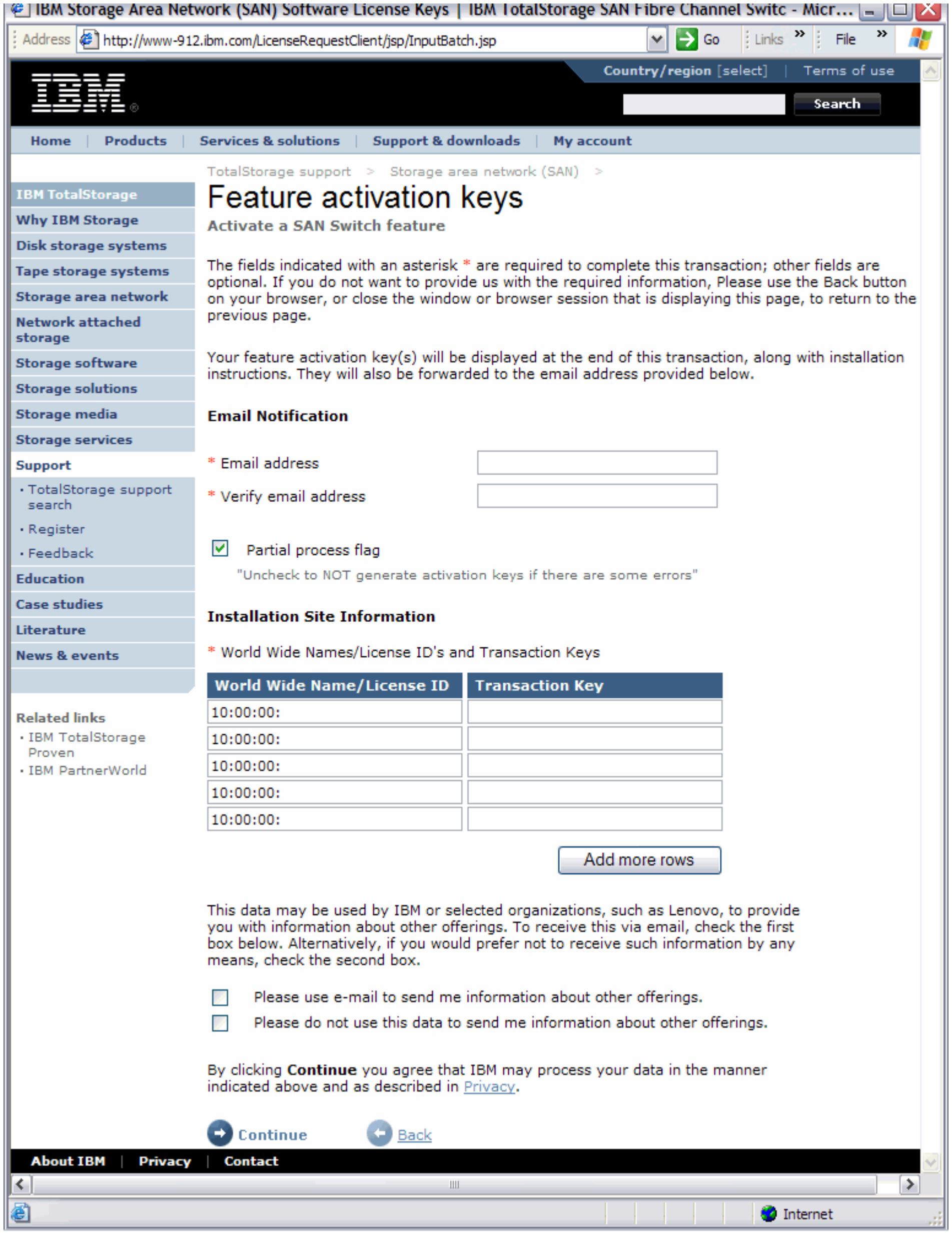
3. If your switch is a model with a front panel display, the WWN can be shown on this display. Select the following command sequence:

   Status Menu > World Wide Name.

If you have forgotten your password when logging into the switch to get the WWN, the default is 'password'. Try the default to log in. If that does not work, contact your switch administrator for the correct password."

Figure 1-81 Feature activation keys Web site

Clicking the **Generate activation keys** link presents the next page in the **Feature activation keys** series. You must also have your e-mail address and your transaction key(s) available. See Figure 1-82.


IBM Storage Area Network (SAN) Software License Keys | IBM TotalStorage SAN Fibre Channel Switc - Micr...
Address
http://www-912.ibm.com/LicenseRequestClient/jsp/InputBatch.jsp
Go
Links
File
IBM
Country/region [select]
Terms of use
Search
Home
Products
Services & solutions
Support & downloads
My account
TotalStorage support > Storage area network (SAN) >
IBM TotalStorage
Why IBM Storage
Disk storage systems
Tape storage systems
Storage area network
Network attached storage
Storage software
Storage solutions
Storage media
Storage services
Support
· TotalStorage support search
· Register
· Feedback
Education
Case studies
Literature
News & events
Related links
· IBM TotalStorage Proven
· IBM PartnerWorld
Add more rows
Continue
Back
About IBM
Privacy
Contact
Internet

Feature activation keys

Activate a SAN Switch feature

The fields indicated with an asterisk * are required to complete this transaction; other fields are optional. If you do not want to provide us with the required information, Please use the Back button on your browser, or close the window or browser session that is displaying this page, to return to the previous page.

Your feature activation key(s) will be displayed at the end of this transaction, along with installation instructions. They will also be forwarded to the email address provided below.

Email Notification

* Email address

* Verify email address

☑ Partial process flag

"Uncheck to NOT generate activation keys if there are some errors"

Installation Site Information

* World Wide Names/License ID's and Transaction Keys

World Wide Name/License ID	Transaction Key
10:00:00:	
10:00:00:	
10:00:00:	
10:00:00:	
10:00:00:	

This data may be used by IBM or selected organizations, such as Lenovo, to provide you with information about other offerings. To receive this via email, check the first box below. Alternatively, if you would prefer not to receive such information by any means, check the second box.

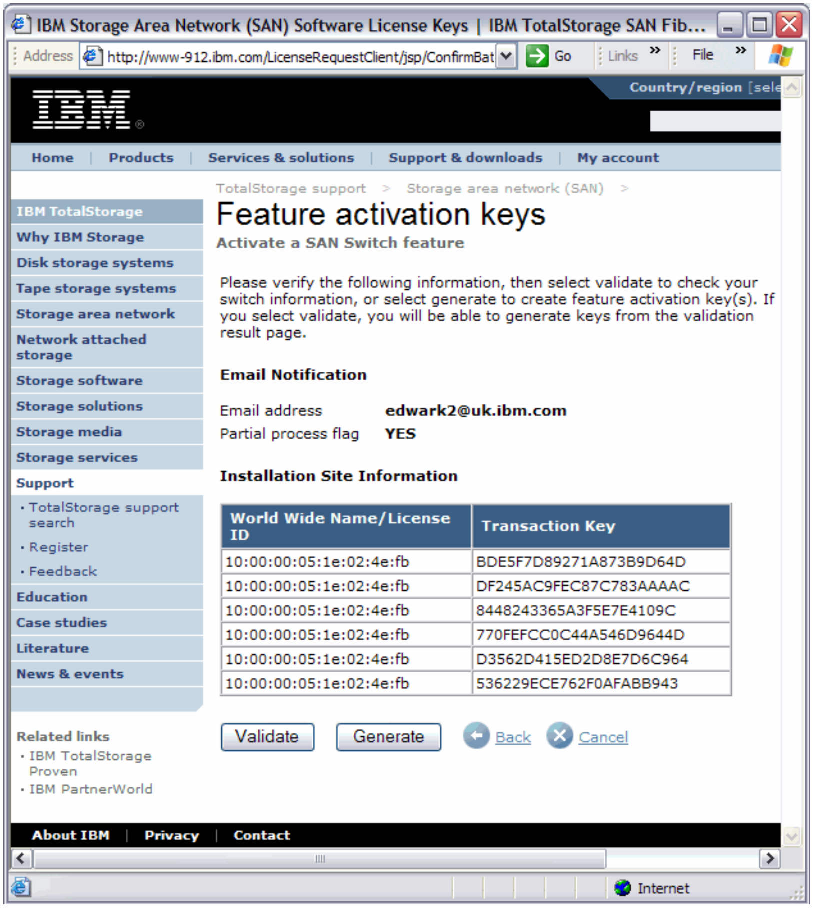
☐ Please use e-mail to send me information about other offerings.

☐ Please do not use this data to send me information about other offerings.

By clicking **Continue** you agree that IBM may process your data in the manner indicated above and as described in Privacy.

Figure 1-82 Feature Activation - WWN/LicenseID plus Transaction Key

Enter your e-mail address, license ID, and the Transaction Key. Notice that the switch license ID should be entered into the World Wide Name/License ID field as shown in Figure 1-83.


IBM Storage Area Network (SAN) Software License Keys | IBM TotalStorage SAN Fib...
Address http://www-912.ibm.com/LicenseRequestClient/jsp/ConfirmBat
Go
Links
File
Country/region [sele
IBM
Home | Products | Services & solutions | Support & downloads | My account
TotalStorage support > Storage area network (SAN) >
IBM TotalStorage
Why IBM Storage
Disk storage systems
Tape storage systems
Storage area network
Network attached storage
Storage software
Storage solutions
Storage media
Storage services
Support
· TotalStorage support search
· Register
· Feedback
Education
Case studies
Literature
News & events
Related links
· IBM TotalStorage Proven
· IBM PartnerWorld
Validate
Generate
Back
Cancel
About IBM | Privacy | Contact
Internet

Feature activation keys

Activate a SAN Switch feature

Please verify the following information, then select validate to check your switch information, or select generate to create feature activation key(s). If you select validate, you will be able to generate keys from the validation result page.

Email Notification

Email address **edwark2@uk.ibm.com**

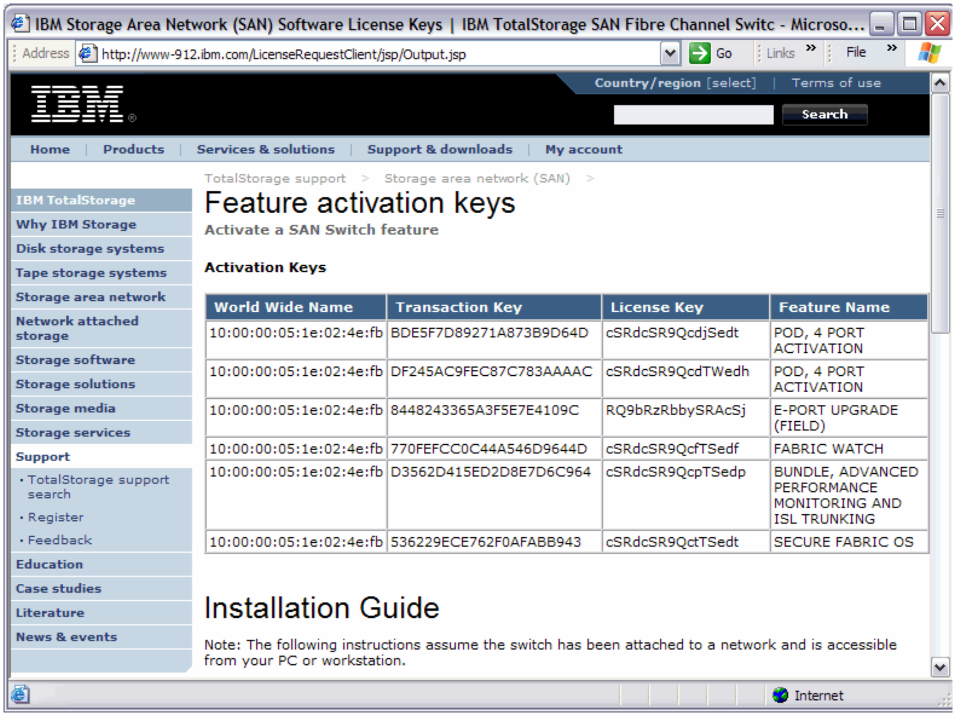
Partial process flag **YES**

Installation Site Information

World Wide Name/License ID	Transaction Key
10:00:00:05:1e:02:4e:fb	BDE5F7D89271A873B9D64D
10:00:00:05:1e:02:4e:fb	DF245AC9FEC87C783AAAAC
10:00:00:05:1e:02:4e:fb	8448243365A3F5E7E4109C
10:00:00:05:1e:02:4e:fb	770FEFCC0C44A546D9644D
10:00:00:05:1e:02:4e:fb	D3562D415ED2D8E7D6C964
10:00:00:05:1e:02:4e:fb	536229ECE762F0AFABB943

Figure 1-83 Feature Activation - Generate keys

After we have completed the details, we click the **`Generate`** button and are then presented with our Activation Keys for our licensed products, as seen in Figure 1-84.


IBM Storage Area Network (SAN) Software License Keys | IBM TotalStorage SAN Fibre Channel Switc - Microso...
Address http://www-912.ibm.com/LicenseRequestClient/jsp/Output.jsp
Go
Links
File
IBM
Country/region [select]
Terms of use
Search
Home
Products
Services & solutions
Support & downloads
My account
IBM TotalStorage
Why IBM Storage
Disk storage systems
Tape storage systems
Storage area network
Network attached storage
Storage software
Storage solutions
Storage media
Storage services
Support
· TotalStorage support search
· Register
· Feedback
Education
Case studies
Literature
News & events
TotalStorage support > Storage area network (SAN) >
Internet

Feature activation keys

Activate a SAN Switch feature

Activation Keys

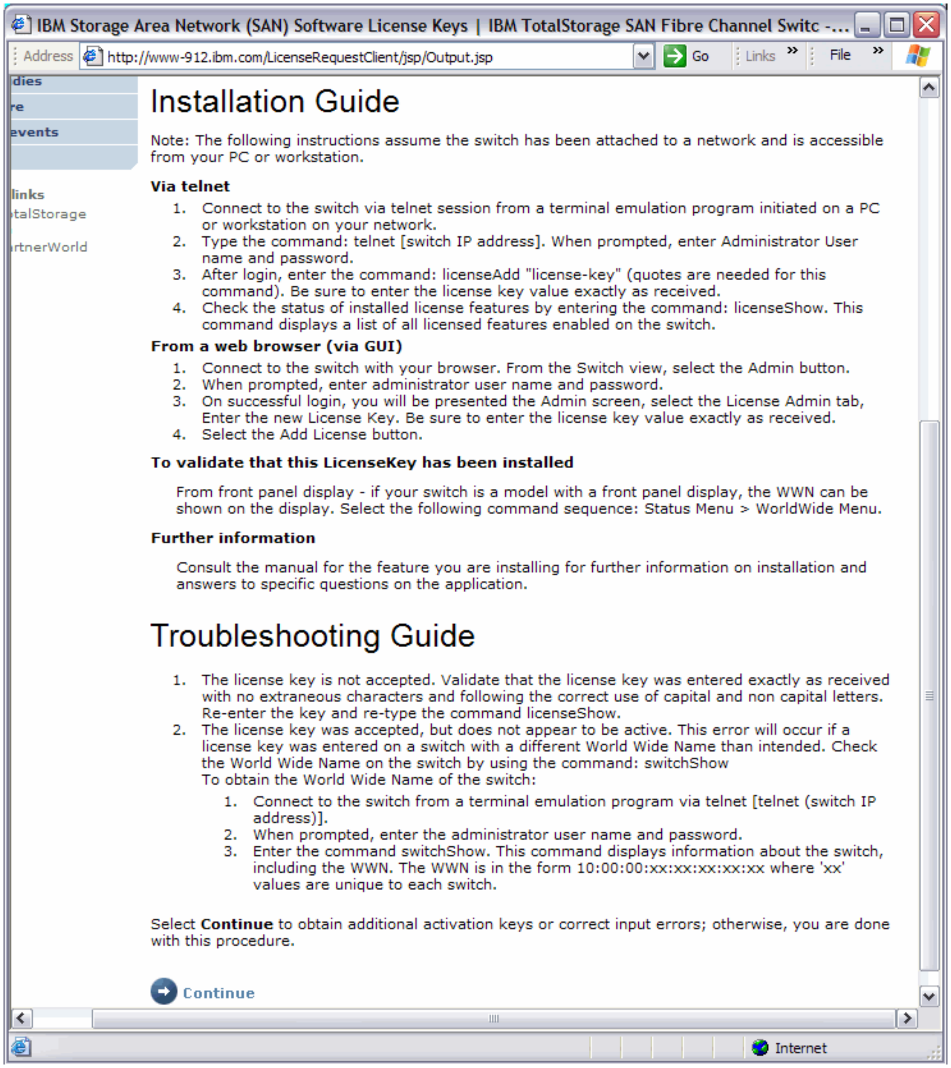
World Wide Name	Transaction Key	License Key	Feature Name
10:00:00:05:1e:02:4e:fb	BDE5F7D89271A873B9D64D	cSRdcSR9QcdjSedt	POD, 4 PORT ACTIVATION
10:00:00:05:1e:02:4e:fb	DF245AC9FEC87C783AAAAC	cSRdcSR9QcdTWedh	POD, 4 PORT ACTIVATION
10:00:00:05:1e:02:4e:fb	8448243365A3F5E7E4109C	RQ9bRzRbbySRAcSj	E-PORT UPGRADE (FIELD)
10:00:00:05:1e:02:4e:fb	770FEFCC0C44A546D9644D	cSRdcSR9QcfTSedf	FABRIC WATCH
10:00:00:05:1e:02:4e:fb	D3562D415ED2D8E7D6C964	cSRdcSR9QcpTSedp	BUNDLE, ADVANCED PERFORMANCE MONITORING AND ISL TRUNKING
10:00:00:05:1e:02:4e:fb	536229ECE762F0AFABB943	cSRdcSR9QctTSedt	SECURE FABRIC OS

Installation Guide

Note: The following instructions assume the switch has been attached to a network and is accessible from your PC or workstation.

Figure 1-84 Feature Activation Keys

This Web page also details the installation process for your license keys, covering both the CLI and GUI options as well as a troubleshooting guide as shown in Figure 1-85.


IBM Storage Area Network (SAN) Software License Keys | IBM TotalStorage SAN Fibre Channel Switc -...
Address http://www-912.ibm.com/LicenseRequestClient/jsp/Output.jsp
Go
Links
File
dies
re
events
links
talStorage
rtnerWorld
Internet

Installation Guide

Note: The following instructions assume the switch has been attached to a network and is accessible from your PC or workstation.

Via telnet

1. Connect to the switch via telnet session from a terminal emulation program initiated on a PC or workstation on your network.
2. Type the command: telnet [switch IP address]. When prompted, enter Administrator User name and password.
3. After login, enter the command: licenseAdd "license-key" (quotes are needed for this command). Be sure to enter the license key value exactly as received.
4. Check the status of installed license features by entering the command: licenseShow. This command displays a list of all licensed features enabled on the switch.

From a web browser (via GUI)

1. Connect to the switch with your browser. From the Switch view, select the Admin button.
2. When prompted, enter administrator user name and password.
3. On successful login, you will be presented the Admin screen, select the License Admin tab, Enter the new License Key. Be sure to enter the license key value exactly as received.
4. Select the Add License button.

To validate that this LicenseKey has been installed

From front panel display - if your switch is a model with a front panel display, the WWN can be shown on the display. Select the following command sequence: Status Menu > WorldWide Menu.

Further information

Consult the manual for the feature you are installing for further information on installation and answers to specific questions on the application.

Troubleshooting Guide

1. The license key is not accepted. Validate that the license key was entered exactly as received with no extraneous characters and following the correct use of capital and non capital letters. Re-enter the key and re-type the command licenseShow.
2. The license key was accepted, but does not appear to be active. This error will occur if a license key was entered on a switch with a different World Wide Name than intended. Check the World Wide Name on the switch by using the command: switchShow
   To obtain the World Wide Name of the switch:
   1. Connect to the switch from a terminal emulation program via telnet [telnet (switch IP address)].
   2. When prompted, enter the administrator user name and password.
   3. Enter the command switchShow. This command displays information about the switch, including the WWN. The WWN is in the form 10:00:00:xx:xx:xx:xx:xx where 'xx' values are unique to each switch.

Select **Continue** to obtain additional activation keys or correct input errors; otherwise, you are done with this procedure.

Continue

Figure 1-85 Feature Activation Installation Guide

Next we detail the Web Tools GUI followed by the CLI processes.

Adding a license key

We can add a license key as follows:

1. Click **Add** on the license tab. The Add License dialog displays.
2. Paste or type a license key in the field.
3. Click **Add License**.
4. Click **Refresh** to display the new licenses in the License tab.

Removing a license key

To remove a license key, we follow the reverse of the procedure shown above:

1. Highlight the license key to remove.
2. Click **Remove**.
3. Click **Yes** to confirm we are removing the license.
4. Click **Refresh** to show that the license has been removed.

In Table 1-16 we describe the fields on the **License Administration** tab.

Table 1-16 License admin tab

Field	Description
License Key	Enter license key to be added or removed.
Feature(s)	A list of the licenses installed on the switch.
Add	Select to add the specified license.
Remove	Select to remove the specified license.
Close	Select to exit the Admin Window.
Refresh	Click to retrieve current values from the switch.

Installing a license key through the CLI

To install a license key feature using the CLI, perform the following steps:

1. From a command prompt, use the Telnet command to log onto the switch using an account that has administrative privileges. Here, *address* is replaced with the switch IP address. For example:

   ```
   C:\telnet address
   ```

2. To determine which licenses are already installed on the switch, type **`licenseShow`** at the command line. A list displays of all the licenses currently installed on the switch, as shown in Example 1-13.

Example 1-13 licenseshow CLI output from SAN256B

```
IBM_M48_SJC:admin> licenseShow
S9e9Sc9SeQTAfAT2:
    Web license
cRRQSzQeySdSSRTG:
    Zoning license
ybccyyde9zcddzz:
    Fabric license
bzdeyRzRbee0efzr:
    Fabric Watch license
bzdeyRzRbeg0efzt:
    Performance Monitor license
bzdeyRzRbek0efzx:
    Trunking license
bzdeyRzRbes2efz7:
    Security license
    FICON_CUP license
SeSQQ9yQzzTfTRRM:
    Extended Fabric license
bzdeyRzRbec4efzt:
    N_Port ID Virtualization license
bzdeyRzRbec8efzx:
    FCIP license
```

3. To install a license key, enter the following command on the command line:

   ```
   licenseAdd "key"
   ```

   Here, “key” is the license key provided to you, enclosed in double quotes. The license key is case sensitive and must be entered exactly as given.

4. Verify that the license was added by entering the following command on the command line:

   ```
   licenseShow
   ```

   If the license is listed, the feature is installed and immediately available. If the license is not listed, repeat step 3.

In Example 1-14 we add the following licenses to a SAN16B switch:

- E_Port Fabric license
- Fabric Watch license

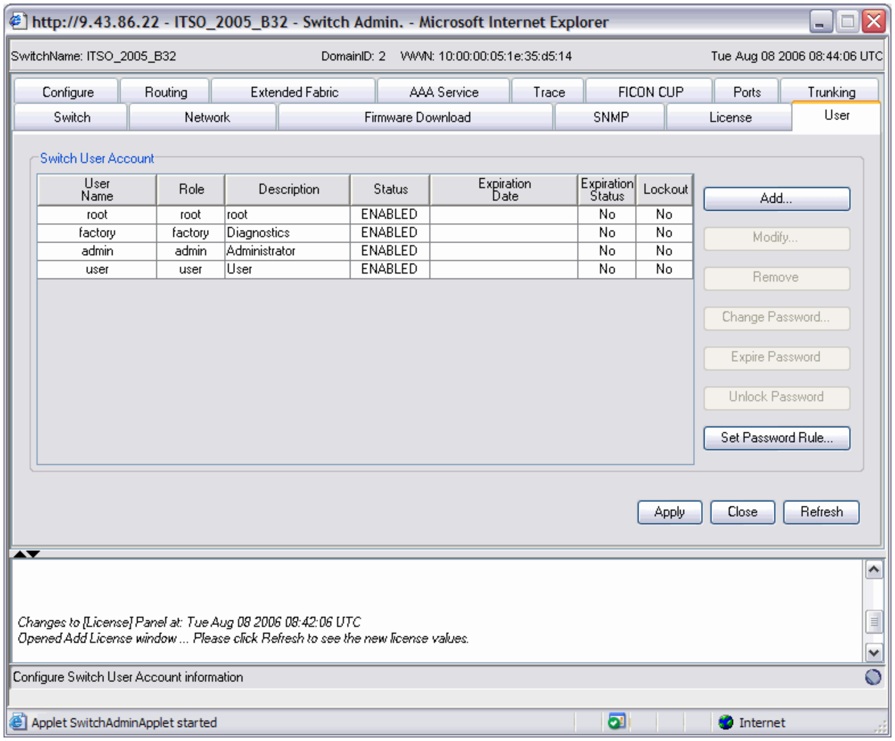
> **Important:** The addition of the E_Port Fabric license *requires* a reboot of the switch. By running the `licenseShow` command before and after our change, we can clearly see the updates.

Example 1-14 Adding licenses

```
Fabric OS (IBM_2005_B16)
Fabos Version 5.1.0b


IBM_2005_B16 login: admin
Password:
IBM_2005_B16:admin> licenseShow
bbSy9dbQSzccTzAg:
    Web license
RycQRyRccSzdRSS:
    Zoning license
cSRdcSR9QcdjSedt:
    Ports on Demand license - additional 4 port upgrade
cSRdcSR9QcdTWedh:
    Ports on Demand license - additional 4 port upgrade

IBM_2005_B16:admin> licenseAdd "RQ9bRzRbbySRAcSj"
adding license-key "RQ9bRzRbbySRAcSj"
For license to take effect, Please reboot the switch now...
IBM_2005_B16:admin> licenseAdd "cSRdcSR9QcfTSedf"
adding license-key "cSRdcSR9QcfTSedf"

IBM_2005_B16:admin> licenseShow
bbSy9dbQSzccTzAg:
    Web license
RycQRyRccSzdRSS:
    Zoning license
cSRdcSR9QcdjSedt:
    Ports on Demand license - additional 4 port upgrade
cSRdcSR9QcdTWedh:
    Ports on Demand license - additional 4 port upgrade
RQ9bRzRbbySRAcSj:
    Fabric license
cSRdcSR9QcfTSedf:
    Fabric Watch license
IBM_2005_B16:admin>
```

User tab

To perform User Administration functions, go to the **User** tab as shown in Figure 1-86.


http://9.43.86.22 - ITSO_2005_B32 - Switch Admin. - Microsoft Internet Explorer
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Ports
Trunking
Switch
Network
Firmware Download
SNMP
License
User
Switch User Account
Add...
Modify...
Remove
Change Password...
Expire Password
Unlock Password
Set Password Rule...
Apply
Close
Refresh
Internet

SwitchName: ITSO_2005_B32 DomainID: 2 WWN: 10:00:00:05:1e:35:d5:14 Tue Aug 08 2006 08:44:06 UTC

User Name	Role	Description	Status	Expiration Date	Expiration Status	Lockout
root	root	root	ENABLED		No	No
factory	factory	Diagnostics	ENABLED		No	No
admin	admin	Administrator	ENABLED		No	No
user	user	User	ENABLED		No	No

Changes to [License] Panel at: Tue Aug 08 2006 08:42:06 UTC
Opened Add License window ... Please click Refresh to see the new license values.

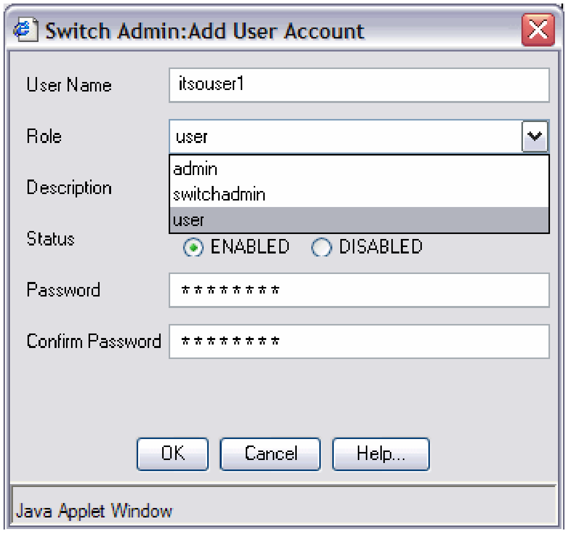
Configure Switch User Account information

Applet SwitchAdminApplet started

Figure 1-86 Users Account Information

From this window, we can manage the User accounts that allow access to the switches from the TotalStorage Switch Specialist.

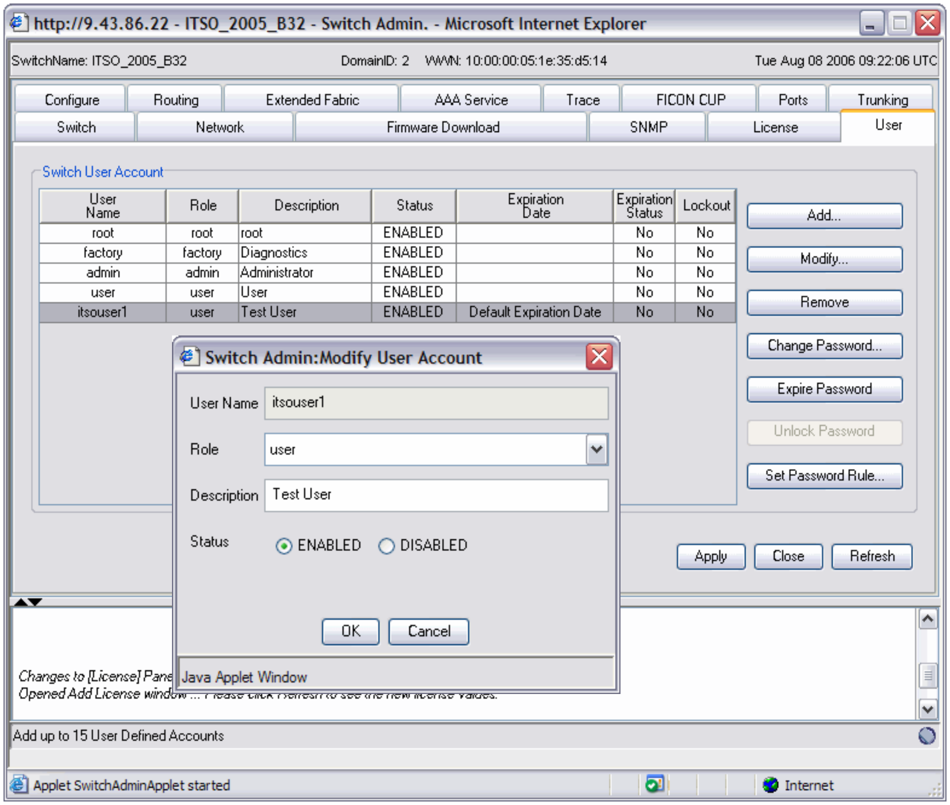
To add a new user, click the **Add** button and the Switch Admin:Add User Account window appears as shown Figure 1-87. When the new user is added, select the proper authority level and decide if it should be enabled or disabled. For our purposes, we have enabled this user account when adding it.


Switch Admin:Add User Account
admin
switchadmin
user
OK
Cancel
Help...
Java Applet Window

User Name: itsouser1
Role: user
Description
Status: ● ENABLED ○ DISABLED
Password: ********
Confirm Password: ********

Figure 1-87 Add new user

To enable/disable a user account, we highlight the User name and click the **Modify** button. A window pops up as shown in Figure 1-88. Here, we click the **Enable** or **Disable** radio button as required and then click **OK**.



http://9.43.86.22 - ITSO_2005_B32 - Switch Admin. - Microsoft Internet Explorer

SwitchName: ITSO_2005_B32 DomainID: 2 WWN: 10:00:00:05:1e:35:d5:14 Tue Aug 08 2006 09:22:06 UTC

Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Ports
Trunking
Switch
Network
Firmware Download
SNMP
License
User
Switch User Account

User Name	Role	Description	Status	Expiration Date	Expiration Status	Lockout
root	root	root	ENABLED		No	No
factory	factory	Diagnostics	ENABLED		No	No
admin	admin	Administrator	ENABLED		No	No
user	user	User	ENABLED		No	No
itsouser1	user	Test User	ENABLED	Default Expiration Date	No	No

Add...
Modify...
Remove
Change Password...
Expire Password
Unlock Password
Set Password Rule...
Apply
Close
Refresh
Switch Admin:Modify User Account

User Name: itsouser1

Role: user

Description: Test User

Status: ● ENABLED ○ DISABLED

OK
Cancel
Java Applet Window

Changes to [License] Pane

Opened Add License window ... Please click Refresh to see the new license values.

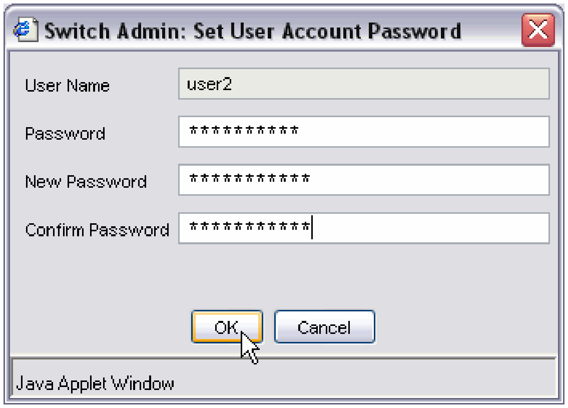
Add up to 15 User Defined Accounts

Applet SwitchAdminApplet started

Figure 1-88 Modify user account status

Restriction: Changing the User Name does *not* create additional users, it is only changing the existing ID to a new name.

If we only want to change the password, we highlight the user and then click the **Change Password** button (Figure 1-89).



Switch Admin: Set User Account Password

User Name: user2

Password: **********

New Password: ***********

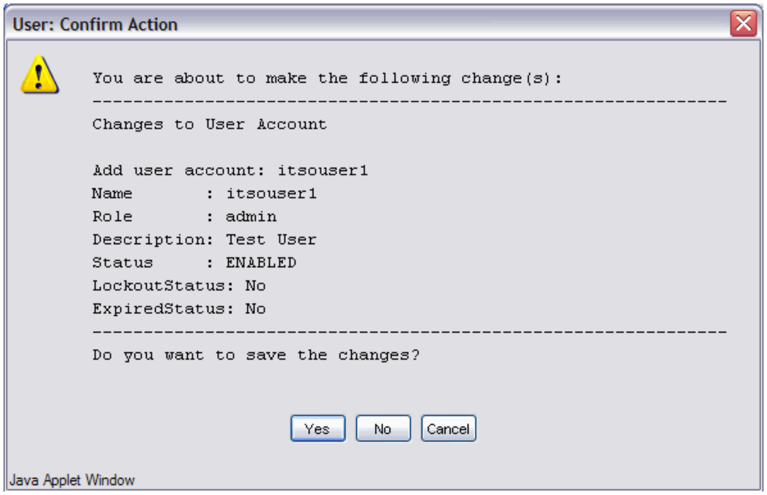
Confirm Password: ***********

Figure 1-89 Changing user password window

At the pop-up window as shown in Figure 1-89, we enter our current password and the new password into *Password* and *Confirm Password* fields. Clicking **OK** validates the changes.

If we want to remove a User account, we highlight the user to select it and then click the **Remove** button.

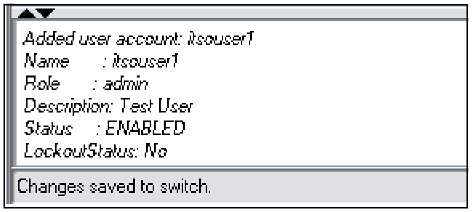
For the changes to be successfully committed to the switch, we must click the **Apply** button. When we do, a window pops up to confirm our actions as shown in Figure 1-90.



```
You are about to make the following change(s):
---------------------------------------------------------------
Changes to User Account

Add user account: itsouser1
Name       : itsouser1
Role       : admin
Description: Test User
Status     : ENABLED
LockoutStatus: No
ExpiredStatus: No
---------------------------------------------------------------
Do you want to save the changes?
```

Figure 1-90 Confirm changes to User accounts

After clicking **Yes**, the changes are committed to the switch. The messages are listed in the report window as shown in Figure 1-91.



```
Added user account: itsouser1
Name       : itsouser1
Role      : admin
Description: Test User
Status     : ENABLED
LockoutStatus: No
Changes saved to switch.
```

Figure 1-91 User account changes report window

Admin access level

This access level allows change and view access to all functions. From telnet access, the Admin level allows use of all commands within the Help Menu. Typically, most switch administration is performed at this level.

User access level

This access level provides view access only. Users are not able to make zoning changes or any switch configuration changes. This level is recommended for monitoring switch activity.

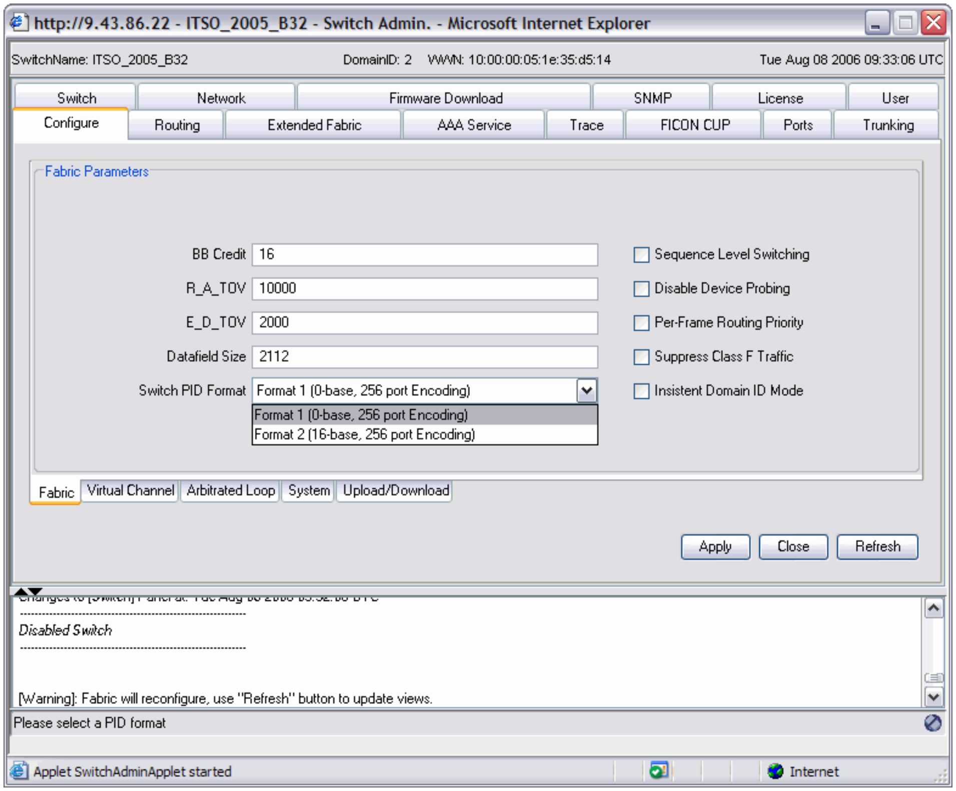
SwitchAdmin access level

This new role has most of the existing permissions of the traditional “admin” role but cannot create/change fabric security policies; cannot create/change fabric zoning policies, and cannot create/manage users.

> **Note:** The User tab does not display or modify the RADIUS host server database.

Configure tab

Clicking the **Configure** tab displays the panel shown in Figure 1-92. We are unable to make any changes to the settings on this tab if the switch is enabled, however the Upload/Download facility is available regardless of the switch status. In the example we have disabled the switch to allow configuration changes to be made.


Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Ports
Trunking
Fabric Parameters
Fabric
Virtual Channel
Arbitrated Loop
System
Upload/Download
Apply
Close
Refresh

http://9.43.86.22 - ITSO_2005_B32 - Switch Admin. - Microsoft Internet Explorer

SwitchName: ITSO_2005_B32 DomainID: 2 WWN: 10:00:00:05:1e:35:d5:14 Tue Aug 08 2006 09:33:06 UTC

BB Credit: 16

R_A_TOV: 10000

E_D_TOV: 2000

Datafield Size: 2112

Switch PID Format: Format 1 (0-base, 256 port Encoding)

- Format 1 (0-base, 256 port Encoding)
- Format 2 (16-base, 256 port Encoding)

☐ Sequence Level Switching

☐ Disable Device Probing

☐ Per-Frame Routing Priority

☐ Suppress Class F Traffic

☐ Insistent Domain ID Mode

```
----------------------------------------------------------------
Disabled Switch
----------------------------------------------------------------


[Warning]: Fabric will reconfigure, use "Refresh" button to update views.
```

Please select a PID format

Applet SwitchAdminApplet started

Internet

Figure 1-92 SAN32B Configure tab

The following paragraphs describe the different parameters found on the sub-tabs shown in Figure 1-92 on page 141.

Fabric parameters

These are the Fabric parameters available:

- **`BB Credit:`** The buffer-to-buffer (BB) credit represents the number of buffers available to attached devices for frame receipt. This value ranges from 1 to 27. Default value is 16.
- **`R_A_TOV:`** The Resource Allocation Time Out Value (R_A_TOV) is displayed in milliseconds. Allocated circuit resources with detected errors are not released until this time value has expired. If the condition is resolved prior to the time out, the internal time out clock resets and waits for the next error condition.
- **`E_D_TOV:`** Error Detect Time Out Value (E_D_TOV) is displayed in milliseconds. This timer is used to flag a potential error condition when an expected response is not received (an acknowledgment or reply in response to packet receipt, for example) within the set time limit. If the time for an expected response exceeds the set value, then an error condition occurs.
- **`Datafield Size:`** The largest data field size in bytes.
- **`Switch PID Format:`** When set to 1, allows 0-base, 256 port addressing that is used for core switches. When set to 2, allows 16-base, 256 port addressing. This parameter must be set the same on all switches in the fabric, for more information refer to “Setting Core PID format” on page 54.
- **`Sequence Level Switching:`** When Sequence Level Switching is enabled, frames of the same sequence from a particular source are transmitted together as a group. When this feature disabled, frames are transmitted interleaved among multiple sequences. Under normal conditions, Sequence Level Switching should be disabled for better performance.
- **`Disable Device Probing:`** When Disable Device Probing is enabled, devices that do not register with the Name Server are not present in the Name Server data base. Set this mode only if the switch N_Port discovery process (PLOGI, PRLI, INQUIRY) causes an attached device to fail.
- **`Per-Frame Routing Priority:`** In addition to the eight virtual channels used in frame routing priority, support is also available for per-frame-based prioritization when this value is set. When Per-Frame Route Priority is enabled, the virtual channel ID is used in conjunction with a frame header to form the final virtual channel ID.
- **`Suppress Class F Traffic:`** When enabled, all class F interswitch frames are transmitted as class 2 frames. This is to support remote fabrics which involve ATM gateways which don't support class F traffic.

- **`Insistent Domain ID Mode:`** Setting this mode makes the current domain ID insistent across reboots, power cycles and failover. This is required fabric wide to transmit FICON data.

Virtual Channels parameters

This feature enables fine tuning of ISLs by configuring parameters for the eight virtual channels. These parameters are used for congestion control. We recommend keeping the default values for these parameters unless expert advice is available.

Arbitrated Loop parameters

These are the Arbitrated Loop parameters:

- **`Send Fan Frames:`** Specifies that fabric address notification (FAN) frames be sent to public loop devices to notify them of their node ID and address. When enabled, frames are sent; when disabled, frames are not sent.
- **`Always send RSCN:`** Following the completion of loop initialization, a remote state change notification (RSCN) is issued when FL_Ports detect the presence of new devices or the absence of pre-existing devices. When this mode is enabled, a RSCN is issued upon completion of loop initialization, regardless of the presence or absence of new or preexisting devices.
- **`Do Not Allow AL_PA 0x00:`** This option disallows AL_PA values from being 0.

System Services parameter

The System Services parameter lets you set activity monitoring on the switch:

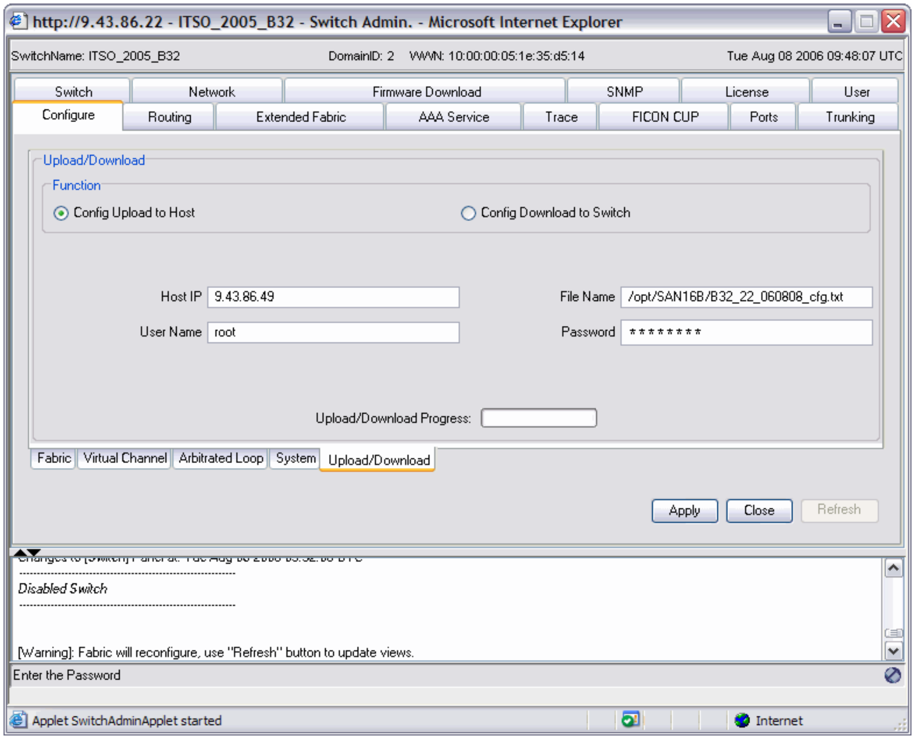
- **`Disable RLS probing:`** Allows you to disable Read Link Error Status of the AL_PAs.

The following options were also available in FOS 5.0.1 and earlier but are no longer available in FOS 5.1.0:

- **`rstatd:`** Allows you to dynamically enable or disable a server that returns details about system operation information through remote procedure calls (RPCs). Be aware that only Ethernet statistics and system up time are supported. The retrieval of this information is supported by a number of operating systems. For example, most UNIX-based systems use the **`rup`** or **`rsysinfo`** command to retrieve the information.
- **`rapid:`** Allows you to dynamically enable or disable a service that handles RPC requests for the API server.
- **`rusersd:`** Allows you to dynamically enable or disable a server that returns information about the user logged into the system through RPC. The retrieval of this information is supported by a number of operating systems. For example, most UNIX-based systems use the **`rusers`** command to retrieve the information.

Upload/download

The functions on the **Configure** tab now allow us to save our configuration file as shown in Figure 1-93.



http://9.43.86.22 - ITSO_2005_B32 - Switch Admin. - Microsoft Internet Explorer

SwitchName: ITSO_2005_B32 DomainID: 2 WWN: 10:00:00:05:1e:35:d5:14 Tue Aug 08 2006 09:48:07 UTC

Upload/Download

Function

● Config Upload to Host ○ Config Download to Switch

Host IP 9.43.86.49

User Name root

File Name /opt/SAN16B/B32_22_060808_cfg.txt

Password ********

Upload/Download Progress:

Disabled Switch

[Warning]: Fabric will reconfigure, use "Refresh" button to update views.

Enter the Password

Applet SwitchAdminApplet started

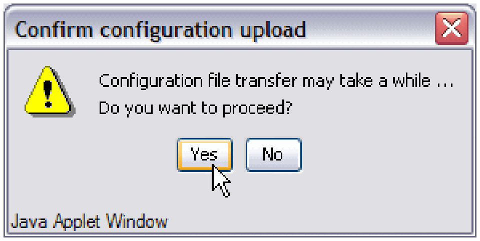
Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Ports
Trunking
Fabric
Virtual Channel
Arbitrated Loop
System
Upload/Download
Apply
Close
Refresh
Internet

Figure 1-93 SAN32B Configure tab to upload configuration file

Notice that when we back up the configuration file for the M12 or the M14, they are saved as two logical switch configurations, so that *both* logical switches must have each configuration file backed up.

To upload the configuration file, click **Config Upload to Host**, provide the host IP address, file name of configuration file, user name and password, and click **Apply**. Remember to use a sensible naming convention for your configuration files to ensure that you are able to recover to the appropriate point as required.

We are prompted to verify that we want to perform this function, as shown in Figure 1-94. We click **Yes** to continue.



Configuration file transfer may take a while ...
Do you want to proceed?

Figure 1-94 Confirm configuration upload

When completed, the confirmation message for the upload appears on the report window.

Routing tab

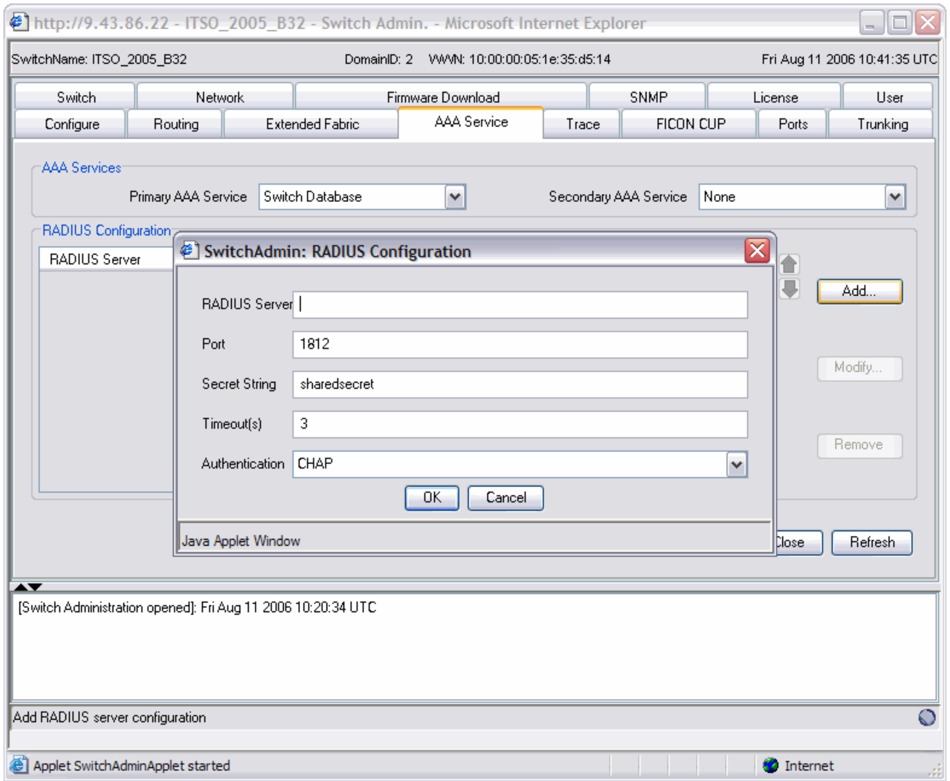
The Routing tab is discussed within the Multiswitch environment in "Routing" on page 325.

Extended Fabric tab

The Extended Fabric tab is also discussed within the Multiswitch environment in "Extended Fabrics within WebTools" on page 318.

AAA tab

From FOS 4.4 onwards, we have support for RADIUS authentication, authorization, and accounting service (known as AAA). When the switch is configured for RADIUS, it becomes a Network Access Server that acts as a RADIUS client. The authentication records are stored in the RADIUS host server database. We can use the AAA tab to manage the RADIUS server as shown in Figure 1-95.



http://9.43.86.22 - ITSO_2005_B32 - Switch Admin. - Microsoft Internet Explorer

SwitchName: ITSO_2005_B32 DomainID: 2 WWN: 10:00:00:05:1e:35:d5:14 Fri Aug 11 2006 10:41:35 UTC

Primary AAA Service: Switch Database

Secondary AAA Service: None

SwitchAdmin: RADIUS Configuration

RADIUS Server:

Port: 1812

Secret String: sharedsecret

Timeout(s): 3

Authentication: CHAP

[Switch Administration opened]: Fri Aug 11 2006 10:20:34 UTC

Add RADIUS server configuration

Applet SwitchAdminApplet started

Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Ports
Trunking
AAA Services
RADIUS Configuration
RADIUS Server
Add...
Modify...
Remove
OK
Cancel
Java Applet Window
Close
Refresh
Internet

Figure 1-95 Adding a RADIUS server from the AAA tab

To add a new RADIUS server, click the **Add** button and fill in the RADIUS server with a valid IP address or DNS string. The other fields are optional and are automatically filled in as shown in Figure 1-95. After we fill in the IP address, we click **OK**.

> **Note:** Each server must have a unique IP address or DNS name.

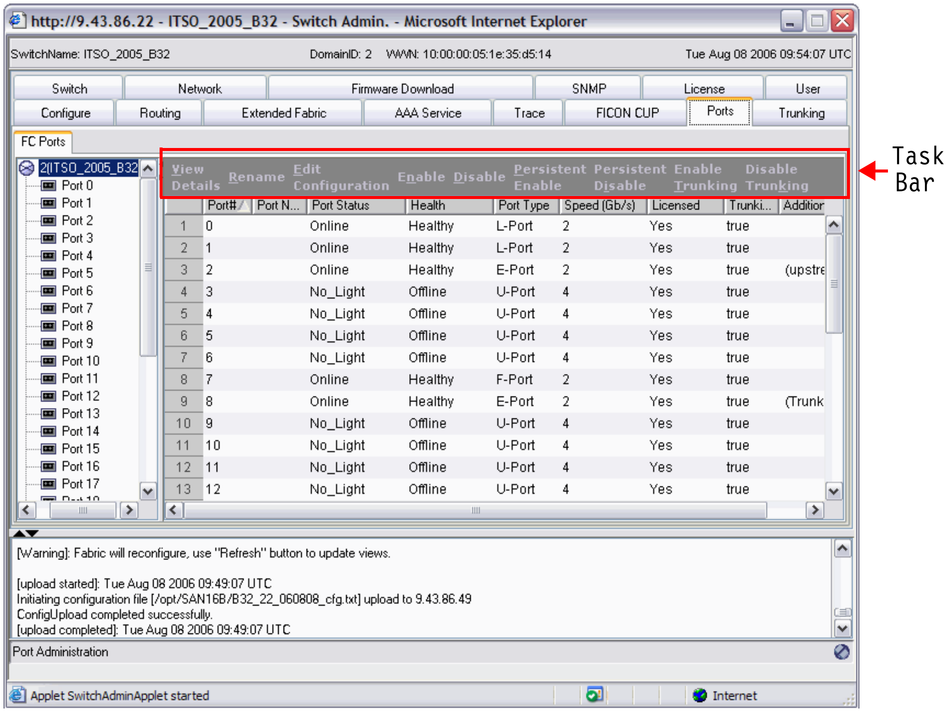
Now that the servers are defined, we can modify or remove them by highlighting them and clicking either **Modify** or **Remove**. When we have finished listing all the servers in the configuration, we can now change the order in which they are contacted for authentication by using the up and down arrow on the right of the window displaying the list of servers. Details are described in Table 1-17.

Table 1-17 AAA tab functionsPorts tab

Function	Description
Primary AAA Service	Primary Service Engine
Secondary AAA Service	A Backup Service Engine
RADIUS configuration	Window displaying RADIUS servers in the configuration
Port	Port for which RADIUS server is defined
Timeout(s)	Timeout value in minutes
Authentication	Authentication protocol used
Up/Down Arrows	Navigate order for which servers are contacted
Add	Add a new RADIUS server
Modify	Modify an existing RADIUS server
Remove	Remove an existing RADIUS server
Apply	Apply and commit changes to the switch
Close	Close the Administration window
Refresh	Refresh the view from the current switch data

Ports tab

Clicking the **Ports** tab displays the panel shown in Figure 1-96.


http://9.43.86.22 - ITSO_2005_B32 - Switch Admin. - Microsoft Internet Explorer
Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Ports
Trunking
FC Ports
2(ITSO_2005_B32
Port 0
Port 1
Port 2
Port 3
Port 4
Port 5
Port 6
Port 7
Port 8
Port 9
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15
Port 16
Port 17
View Details
Rename
Edit Configuration
Enable
Disable
Persistent Enable
Persistent Disable
Enable Trunking
Disable Trunking
Task Bar
Port Administration
Applet SwitchAdminApplet started
Internet

SwitchName: ITSO_2005_B32 DomainID: 2 WWN: 10:00:00:05:1e:35:d5:14 Tue Aug 08 2006 09:54:07 UTC

	Port#	Port N...	Port Status	Health	Port Type	Speed (Gb/s)	Licensed	Trunki...	Addition
1	0		Online	Healthy	L-Port	2	Yes	true	
2	1		Online	Healthy	L-Port	2	Yes	true	
3	2		Online	Healthy	E-Port	2	Yes	true	(upstre
4	3		No_Light	Offline	U-Port	4	Yes	true	
5	4		No_Light	Offline	U-Port	4	Yes	true	
6	5		No_Light	Offline	U-Port	4	Yes	true	
7	6		No_Light	Offline	U-Port	4	Yes	true	
8	7		Online	Healthy	F-Port	2	Yes	true	
9	8		Online	Healthy	E-Port	2	Yes	true	(Trunk
10	9		No_Light	Offline	U-Port	4	Yes	true	
11	10		No_Light	Offline	U-Port	4	Yes	true	
12	11		No_Light	Offline	U-Port	4	Yes	true	
13	12		No_Light	Offline	U-Port	4	Yes	true	

```
[Warning]: Fabric will reconfigure, use "Refresh" button to update views.

[upload started]: Tue Aug 08 2006 09:49:07 UTC
Initiating configuration file [/opt/SAN16B/B32_22_060808_cfg.txt] upload to 9.43.86.49
ConfigUpload completed successfully.
[upload completed]: Tue Aug 08 2006 09:49:07 UTC
```

Figure 1-96 SAN32B Port settings tab

The task bar displays the functions that you can perform on the selected port. If you select more than one port, only the tasks that you can perform on all of the selected ports are available. Tasks that are not applicable to the selected ports are greyed out.

On the SAN256B we have a slightly different display in which we can select both the FC and GigE ports as shown in Figure 1-97.

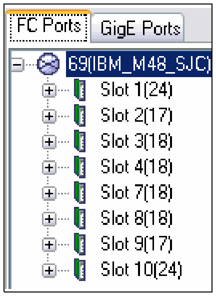


Figure 1-97 M48 Ports tab

From the Ports tab, we can perform the following functions:

- Rename a port.
- Set or reset a persistent Disable per port.
- Disable or enable a specific port.
- Disable or enable trunking for a specific port (default value is enabled).
- View the current port state.
- View the current speed for the switch ports.
- Manually set the speed for a specific port.
- Define a symbolic name to identify what is attached to the port.

Table 1-18 describes the fields on the **Ports tab**.

Table 1-18 Ports details

Field	Description
Port Number	The port number.
Licensed Port	For B32 models shows which ports are licensed. As additional ports are installed and licensed, this field reflects that the new ports are licensed.
L-Port	Check to allow the port to become an L-Port
F-Port	Check to allow the port to become an F-Port
E-Port	Check to allow the port to become an E-Port
Current Type	Shows the current port type. U-Port, F-Port, FL-Port
Enable Trunking	Check to enable the port trunking. Four trunk ports form a group with one of them in the role of master port.

Field	Description
Enable Port	Check to disable the port, uncheck to enable. At power on or reboot, the port is enabled.
Persistent Disable	Check to disable port, remains disabled through switch reboots and power cycles. Uncheck to enable the port.
Port State	Displays the current state of each port (online or no light).
Current Speed	Displays the speed of the port connection. 1G, 2G, 4G as set speeds and N1, N2 or N4 as negotiated speeds.
Change Speed	To change the speed, for example, from negotiated to set speed.
Port Name	Click here to assign a symbolic name to the port.
Apply	Apply and commit the changes to the switch.
Close	Close the administration window
Refresh	Refresh the view with the most recent information from switch.

FICON tab

The FICON CUP tab within WebTools is discussed in 1.11.1, “FICON servers” on page 340.

Trunking tab

The Trunking tab is discussed in “Trunking” on page 311.

1.8.13 Telnet button

All IBM TotalStorage SAN Switches have a Telnet interface that is accessed by clicking the picture of the monitor from the Web Switch view. The Telnet icon is consistent across all of the switches, and in Figure 1-98, we show the SAN256B panel.

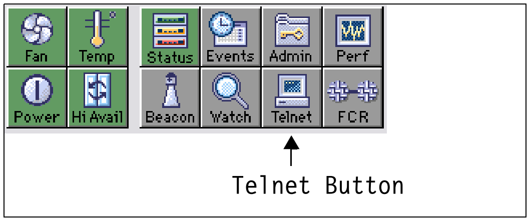
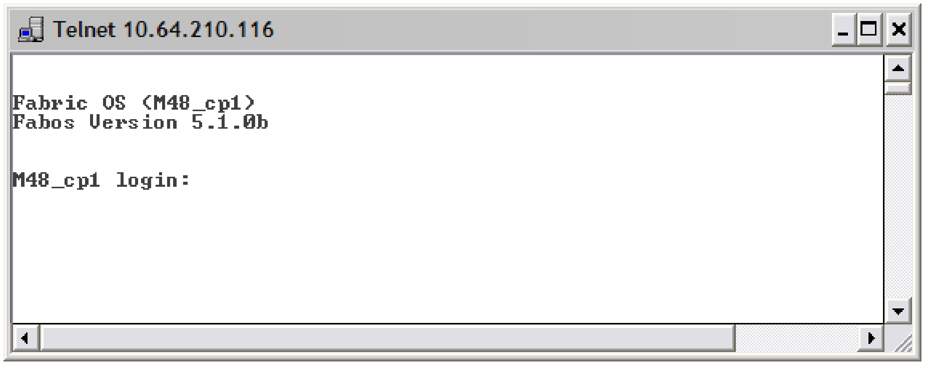


Figure 1-98 SAN256B showing the Telnet button

In Figure 1-99 we show the Telnet window that is presented. At this window, the login and password are required.


Telnet 10.64.210.116

```
Fabric OS (M48_cp1)
Fabos Version 5.1.0b

M48_cp1 login:
```

Figure 1-99 M48 Telnet session

1.8.14 Beaconing button

The Beaconing function allows you to physically locate a switch by sending a signal to the specified switch, which causes an LED yellow light pattern to flash from side to side on the switch. This makes the switch very easy to find.

To activate Beaconing, click the lighthouse icon on the Switch View for the M48, as shown in Figure 1-100.

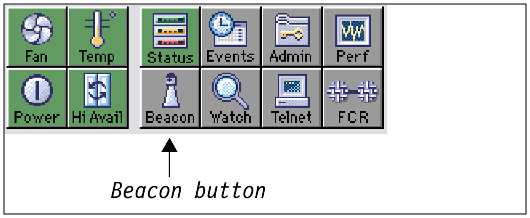
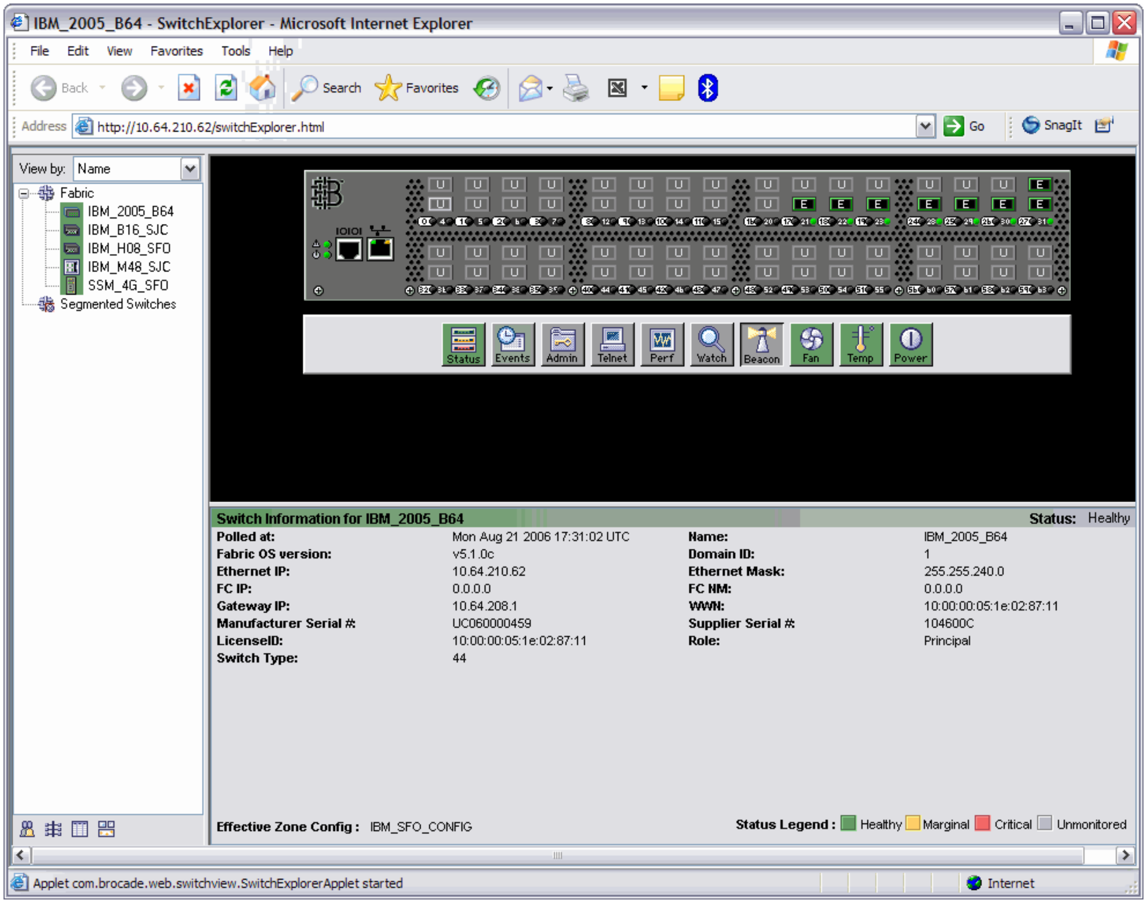

Fan
Temp
Status
Events
Admin
Perf
Power
Hi Avail
Beacon
Watch
Telnet
FCR
Beacon button

Figure 1-100 SAN256B showing the Beaconing button

This function can be toggled on and off once the switch is identified.

Figure 1-101 shows the Web tools view of a SAN64B switch with Beaconing activated.


IBM_2005_B64 - SwitchExplorer - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://10.64.210.62/switchExplorer.html
Go
SnagIt
View by:
Name
Fabric
IBM_2005_B64
IBM_B16_SJC
IBM_H08_SFO
IBM_M48_SJC
SSM_4G_SFO
Segmented Switches
Status
Events
Admin
Telnet
Perf
Watch
Beacon
Fan
Temp
Power

Switch Information for IBM_2005_B64 Status: Healthy

Polled at: Mon Aug 21 2006 17:31:02 UTC
Fabric OS version: v5.1.0c
Ethernet IP: 10.64.210.62
FC IP: 0.0.0.0
Gateway IP: 10.64.208.1
Manufacturer Serial #: UC060000459
LicenseID: 10:00:00:05:1e:02:87:11
Switch Type: 44
Name: IBM_2005_B64
Domain ID: 1
Ethernet Mask: 255.255.240.0
FC NM: 0.0.0.0
WWN: 10:00:00:05:1e:02:87:11
Supplier Serial #: 104600C
Role: Principal

Effective Zone Config : IBM_SFO_CONFIG

Status Legend : 🟩 Healthy 🟨 Marginal 🟥 Critical ☐ Unmonitored

Applet com.brocade.web.switchview.SwitchExplorerApplet started

Internet

Figure 1-101 SAN64B switch with beaconing activated

1.8.15 Performance Monitor button

The basic-mode Performance Monitor is standard in the Web Tools software. However, the Advanced Monitoring menu is an optionally licensed software. The Performance Monitor performs the following functions:

- It graphically displays throughput (megabytes per second) for each port and for the entire switch. Port throughput is the number of bytes that are received at a port plus the number of bytes that are transmitted. Switch throughput is the sum of the throughput for all the ports.

- The Performance Monitor also allows the graphing of traffic based on the Source ID and the Destination ID hardware-filtering mechanism.

To access the Performance Monitor, we click the **Perf** button from the SAN256B switch view in WebTools as shown in Figure 1-102.

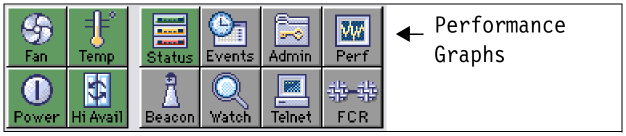


Figure 1-102 M48 Performance Graphs button

The Performance Monitor allows the creation of a collection of graphs which can be viewed on the display panel, or canvas. You can manage this display using the Window drop down menu which allows you to cascade or tile the graphs.

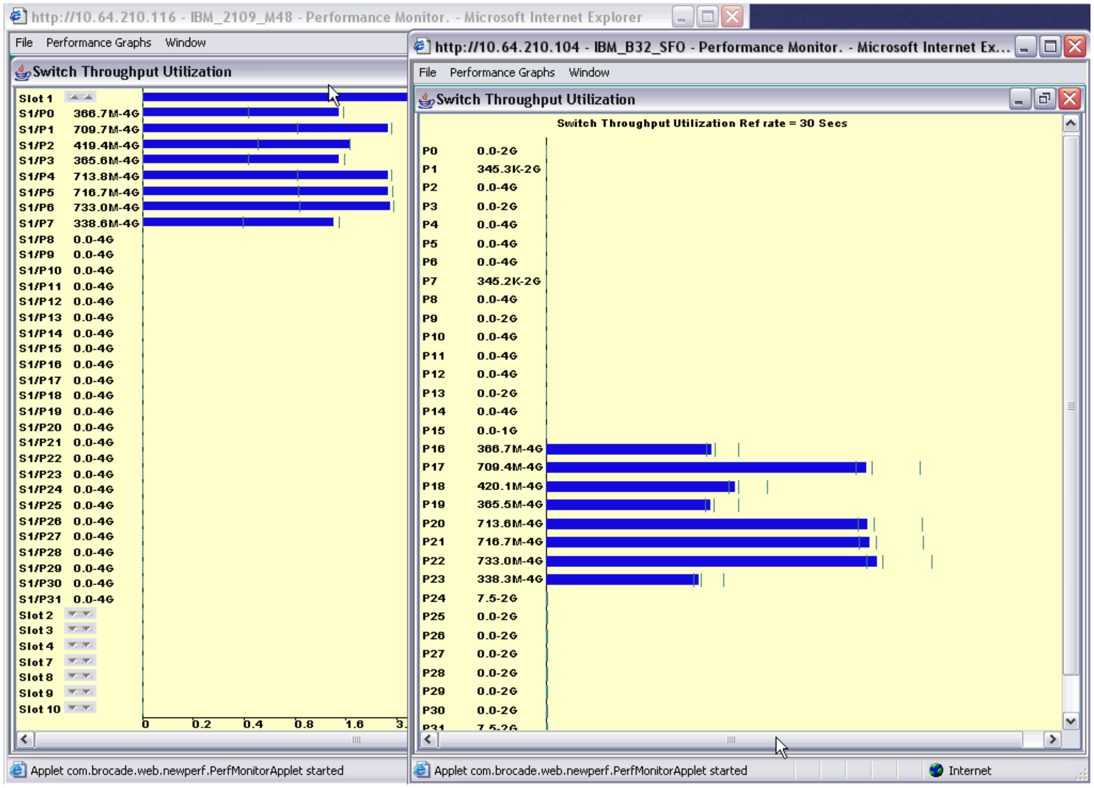
Performance monitoring allows us to manage and balance the workload across our SAN, enabling us to make performance improvements and also assisting with capacity planning.

Features

These are some of the features available in the Performance Monitor:

- An existing report can be selected from the predefined list.
- In some cases, you can supply the object to be monitored and graphed (such as port number, SID/DID pair, AL_PA, or switch domain number).
- Graphs are displayed on a canvas, which can hold a maximum of eight graphs simultaneously. An individual graph can be maximized to occupy the entire canvas. The size of the graphs on the canvas is determined by the number of graphs being displayed. The window does not have to be scrolled to view all the selected graphs.
- The collection of graphs in the canvas can be stored for later retrieval on the switch. Up to 20 individual canvases can be saved. Each canvas is saved with its name, a brief description, and the graphs that comprise the canvas.
- To print an individual graph, right-click the graph and select print from the menu. Alternatively, you can print all the graphs by selecting **Print All Graphs** from the File menu.

After clicking the **Perf** button from the Switch View, we see the default performance graph as shown in Figure 1-103.


http://10.64.210.116 - IBM_2109_M48 - Performance Monitor. - Microsoft Internet Explorer
File
Performance Graphs
Window
Switch Throughput Utilization
Slot 1
S1/P0 366.7M-4G
S1/P1 709.7M-4G
S1/P2 419.4M-4G
S1/P3 365.6M-4G
S1/P4 713.8M-4G
S1/P5 716.7M-4G
S1/P6 733.0M-4G
S1/P7 338.6M-4G
S1/P8 0.0-4G
S1/P9 0.0-4G
S1/P10 0.0-4G
S1/P11 0.0-4G
S1/P12 0.0-4G
S1/P13 0.0-4G
S1/P14 0.0-4G
S1/P15 0.0-4G
S1/P16 0.0-4G
S1/P17 0.0-4G
S1/P18 0.0-4G
S1/P19 0.0-4G
S1/P20 0.0-4G
S1/P21 0.0-4G
S1/P22 0.0-4G
S1/P23 0.0-4G
S1/P24 0.0-4G
S1/P25 0.0-4G
S1/P26 0.0-4G
S1/P27 0.0-4G
S1/P28 0.0-4G
S1/P29 0.0-4G
S1/P30 0.0-4G
S1/P31 0.0-4G
Slot 2
Slot 3
Slot 4
Slot 7
Slot 8
Slot 9
Slot 10
0
0.2
0.4
0.8
1.6
3.
http://10.64.210.104 - IBM_B32_SFO - Performance Monitor. - Microsoft Internet Ex...
File
Performance Graphs
Window
Switch Throughput Utilization
Switch Throughput Utilization Ref rate = 30 Secs
P0 0.0-2G
P1 345.3K-2G
P2 0.0-4G
P3 0.0-2G
P4 0.0-4G
P5 0.0-4G
P6 0.0-4G
P7 345.2K-2G
P8 0.0-4G
P9 0.0-2G
P10 0.0-4G
P11 0.0-4G
P12 0.0-4G
P13 0.0-2G
P14 0.0-4G
P15 0.0-1G
P16 366.7M-4G
P17 709.4M-4G
P18 420.1M-4G
P19 365.5M-4G
P20 713.6M-4G
P21 716.7M-4G
P22 733.0M-4G
P23 338.3M-4G
P24 7.5-2G
P25 0.0-2G
P26 0.0-2G
P27 0.0-2G
P28 0.0-2G
P29 0.0-2G
P30 0.0-2G
P31 7.5-2G
Internet

Applet com.brocade.web.newperf.PerfMonitorApplet started

Applet com.brocade.web.newperf.PerfMonitorApplet started

Figure 1-103 SAN256B and SAN32B Performance Monitoring default graph

All graphs are real-time and are updated every 30 seconds.

Performance Monitor menus

The Performance Monitor provides three menus:

- File menu
- Performance graphs menu
- Window menu

Actions menu

The Actions menu of the Performance Monitor feature, shown in Figure 1-104, is made up of the following sub-menus:

- Display canvas configurations
- Save current canvas configuration
- Print all graphs

A canvas is a collection of predefined graphs. It can be useful to configure these for your systems so that when performance monitoring is required you can easily start up a series of canvases without having to create them manually.

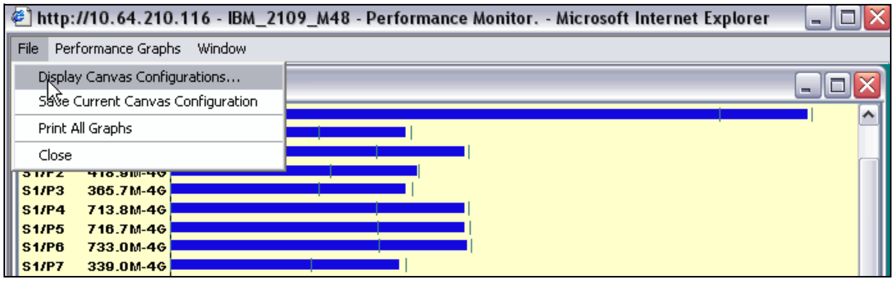
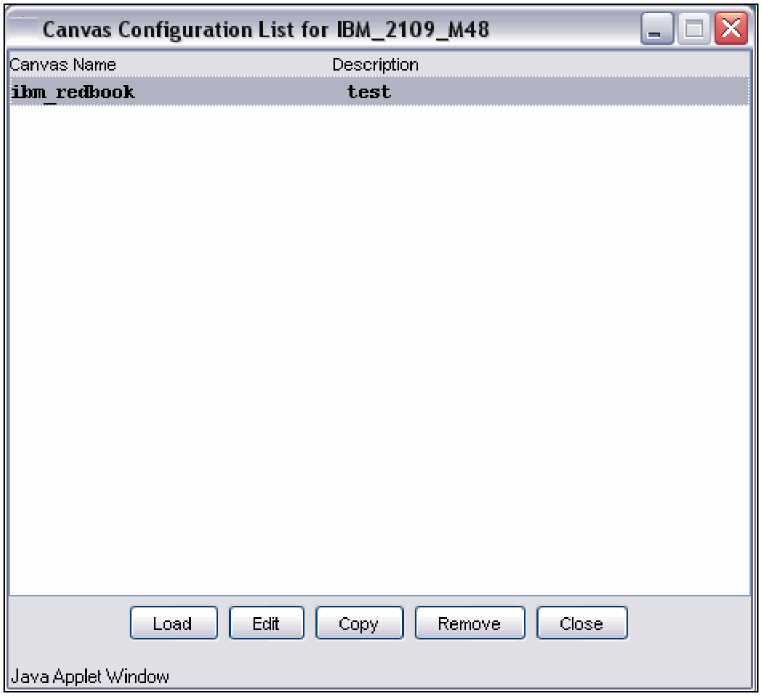

http://10.64.210.116 - IBM_2109_M48 - Performance Monitor. - Microsoft Internet Explorer
File
Performance Graphs
Window
Display Canvas Configurations...
Save Current Canvas Configuration
Print All Graphs
Close
S1/P3 365.7M-4G
S1/P4 713.8M-4G
S1/P5 716.7M-4G
S1/P6 733.0M-4G
S1/P7 339.0M-4G

Figure 1-104 M48 Action Menu selection

Display canvas configurations

Use this item to display and edit the various canvas configurations previously saved, as shown in Figure 1-105.


Canvas Configuration List for IBM_2109_M48
Load
Edit
Copy
Remove
Close
Java Applet Window

Canvas Name	Description
ibm_redbook	test

Figure 1-105 Display canvas configuration

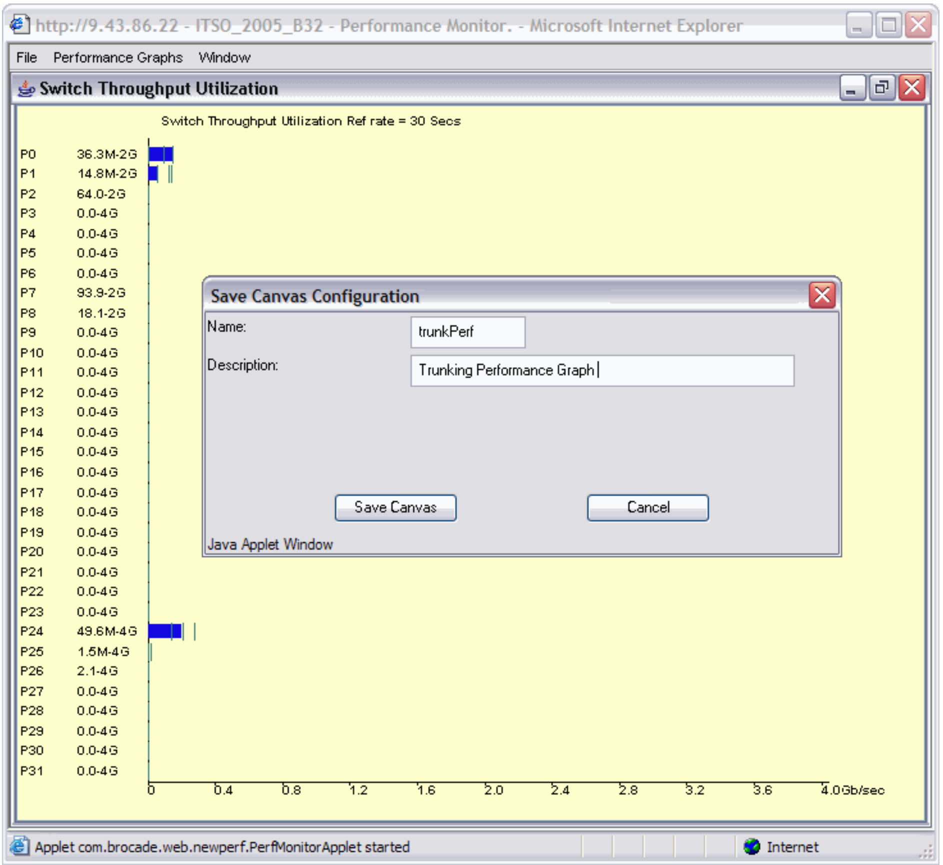
Table 1-19 describes the fields on the Canvas Configuration List window.

Table 1-19 Canvas Configuration List window — fields

Available in Canvas Configuration List	
Load	Select to load a canvas of 1 to 8 graphs onto the Performance Monitor facility by choosing the highlighted canvas name.
Edit	Select to make changes to a canvas or change configurations. A list of graphs which comprise the highlighted canvas appears.
Copy	Select to copy the highlighted canvas configuration from the list to the switch flash. You are prompted to type in the name and description of the canvas to which you want to copy your chosen graph.
Remove	Select to remove a highlighted canvas from the list and the switch flash. You are prompted with a warning that you are going to delete the selected canvas.
Close	Select to close the canvas configuration list.
Available in Edit Canvas Window	
Save	Select to save an edited canvas.
Edit	Select to make changes to a graph on a canvas. A data entry frame appears.
Add	Select to add a graph to a canvas. A pop-up menu of available graphs displays. Use this option to select the type of graph to add. For more information, refer to the *Basic Monitoring* and *Advanced Monitoring* sections of this chapter.
Remove	Select to delete a graph. The graph currently highlighted is removed.
Cancel	Select to exit the window without making any changes.
Available in Copy Canvas List	
Name	Type in the name of the canvas to which you want to copy the graph.
Description	Type in a description of the graph to be copied.
Copy Canvas	Select to copy the selected graph to another canvas.
Cancel	Select to exit the window without making a copy.

Save Current Canvas Configuration

The Save Current Canvas Configuration menu saves the currently configured canvas to the switch. We use a canvas name and a brief description to save the canvas, as shown in Figure 1-106.


http://9.43.86.22 - ITSO_2005_B32 - Performance Monitor. - Microsoft Internet Explorer
File
Performance Graphs
Window
Switch Throughput Utilization
Switch Throughput Utilization Ref rate = 30 Secs
P0 36.3M-2G
P1 14.8M-2G
P2 64.0-2G
P3 0.0-4G
P4 0.0-4G
P5 0.0-4G
P6 0.0-4G
P7 93.9-2G
P8 18.1-2G
P9 0.0-4G
P10 0.0-4G
P11 0.0-4G
P12 0.0-4G
P13 0.0-4G
P14 0.0-4G
P15 0.0-4G
P16 0.0-4G
P17 0.0-4G
P18 0.0-4G
P19 0.0-4G
P20 0.0-4G
P21 0.0-4G
P22 0.0-4G
P23 0.0-4G
P24 49.6M-4G
P25 1.5M-4G
P26 2.1-4G
P27 0.0-4G
P28 0.0-4G
P29 0.0-4G
P30 0.0-4G
P31 0.0-4G
0
0.4
0.8
1.2
1.6
2.0
2.4
2.8
3.2
3.6
4.0Gb/sec
Save Canvas Configuration
Save Canvas
Cancel
Java Applet Window
Internet

Name: trunkPerf

Description: Trunking Performance Graph

Applet com.brocade.web.newperf.PerfMonitorApplet started

Figure 1-106 Saving current canvas selection

If the canvas already exists, the Confirm Override Canvas confirmation window pops up. Use the override option when you have to update an existing canvas. The example we provide includes the switch throughput on port 24, which on our switch is part of a trunking group.

Print all graphs

Use this item to print all the graphs on the selected canvas.

Performance Graphs menu

We show the Performance Graphs menu in Figure 1-107.

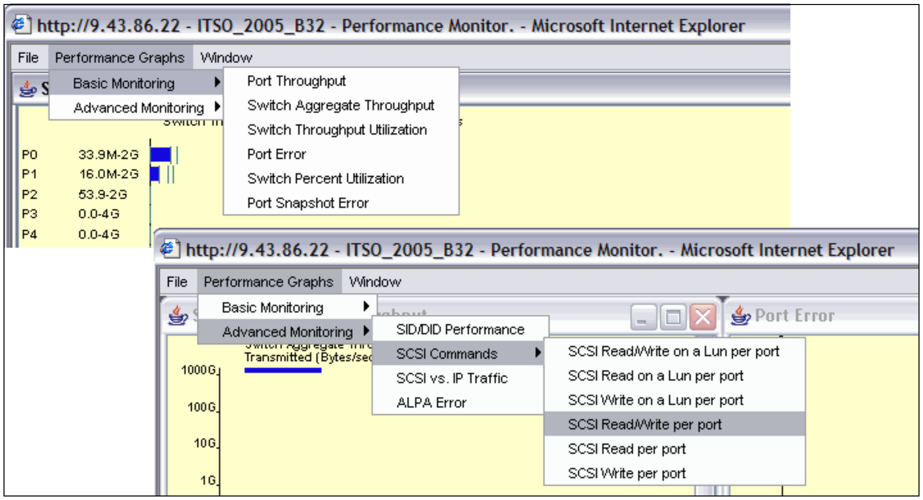

http://9.43.86.22 - ITSO_2005_B32 - Performance Monitor. - Microsoft Internet Explorer
File
Performance Graphs
Window
Basic Monitoring
Advanced Monitoring
Port Throughput
Switch Aggregate Throughput
Switch Throughput Utilization
Port Error
Switch Percent Utilization
Port Snapshot Error
P0 33.9M-2G
P1 16.0M-2G
P2 53.9-2G
P3 0.0-4G
P4 0.0-4G
http://9.43.86.22 - ITSO_2005_B32 - Performance Monitor. - Microsoft Internet Explorer
File
Performance Graphs
Window
Basic Monitoring
Advanced Monitoring
SID/DID Performance
SCSI Commands
SCSI vs. IP Traffic
ALPA Error
SCSI Read/Write on a Lun per port
SCSI Read on a Lun per port
SCSI Write on a Lun per port
SCSI Read/Write per port
SCSI Read per port
SCSI Write per port
Port Error
Transmitted (Bytes/sec
1000G
100G
10G
1G

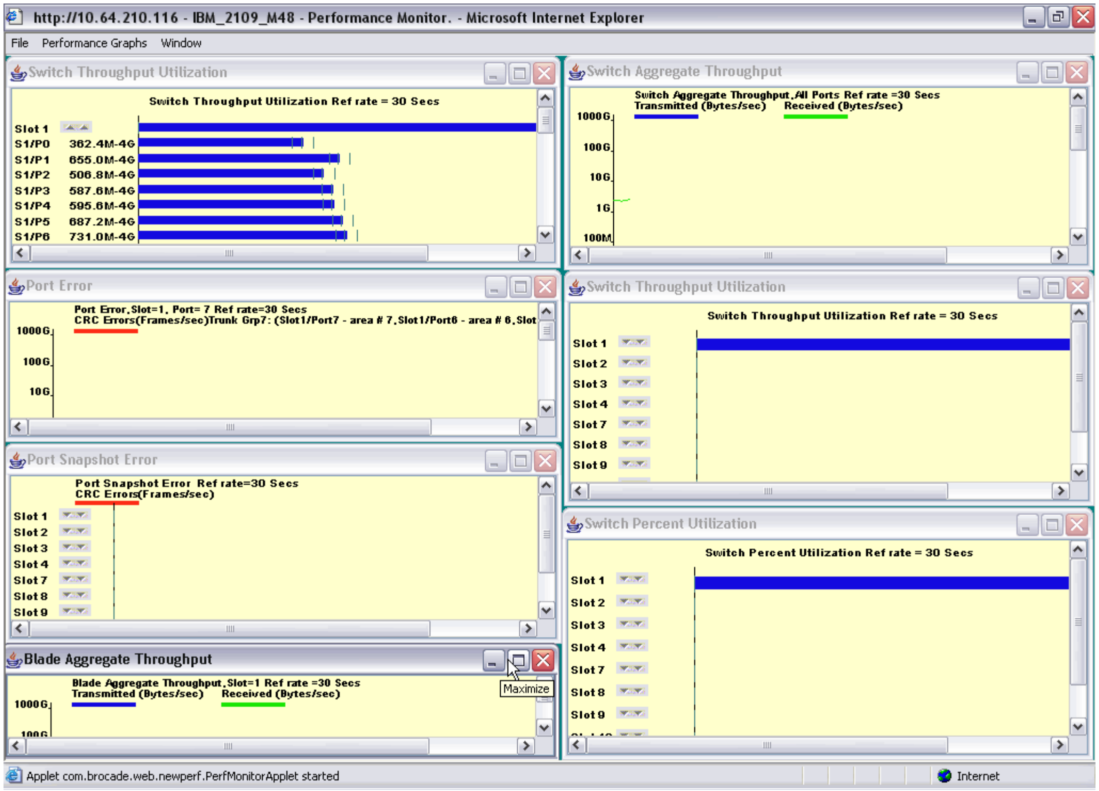
Figure 1-107 Performance Graphs Menu

The Performance Graphs menu gives access to two sets of performance graphs:

- Basic Monitoring
- Advanced Monitoring (requires an additional license key)

Basic Monitoring

We have selected all the options available in basic monitoring and have created a canvas that includes them. This is shown in Figure 1-108.


http://10.64.210.116 - IBM_2109_M48 - Performance Monitor. - Microsoft Internet Explorer
File
Performance Graphs
Window
Switch Throughput Utilization
Switch Throughput Utilization Ref rate = 30 Secs
Slot 1
S1/P0 362.4M-4G
S1/P1 655.0M-4G
S1/P2 508.8M-4G
S1/P3 587.6M-4G
S1/P4 595.6M-4G
S1/P5 687.2M-4G
S1/P6 731.0M-4G
Switch Aggregate Throughput
Switch Aggregate Throughput, All Ports Ref rate =30 Secs
Transmitted (Bytes/sec)
Received (Bytes/sec)
1000G
100G
10G
1G
100M
Port Error
Port Error, Slot=1, Port= 7 Ref rate=30 Secs
CRC Errors(Frames/sec)Trunk Grp7: (Slot1/Port7 - area # 7, Slot1/Port6 - area # 6, Slot
1000G
100G
10G
Switch Throughput Utilization
Switch Throughput Utilization Ref rate = 30 Secs
Slot 1
Slot 2
Slot 3
Slot 4
Slot 7
Slot 8
Slot 9
Port Snapshot Error
Port Snapshot Error Ref rate=30 Secs
CRC Errors(Frames/sec)
Slot 1
Slot 2
Slot 3
Slot 4
Slot 7
Slot 8
Slot 9
Switch Percent Utilization
Switch Percent Utilization Ref rate = 30 Secs
Slot 1
Slot 2
Slot 3
Slot 4
Slot 7
Slot 8
Slot 9
Blade Aggregate Throughput
Blade Aggregate Throughput, Slot=1 Ref rate =30 Secs
Transmitted (Bytes/sec)
Received (Bytes/sec)
1000G
100G
Maximize
Internet

Applet com.brocade.web.newperf.PerfMonitorApplet started

Figure 1-108 Basic monitoring with all functions started

The graphs available on this canvas are described in Table 1-20.

Table 1-20 Graphs available in Basic Monitor

Graph name	Type	Description
Port Throughput Graph	Line	Displays the performance of a port based on four-byte frames received and transmitted.
Switch Aggregate Throughput Graph	Line	Displays the aggregate performance of all ports of a switch. S
Blade Aggregate Throughput Graph (see note below)	Line	Displays the aggregate performance of the ports on a given blade.
Switch Throughput Utilization Graph	Horizontal Bar	Displays the port throughput at the time the sample is taken.
Port Error Graph	Line	Displays a line of CRC errors for a given port.
Switch Percent Utilization Graph	Horizontal Bar	Displays the percentage of usage of a chosen switch at the time the sample is taken.
Ports SnapShot Error Graph	Vertical Bar	Displays the CRC error count between sampling periods for all the ports on a switch.

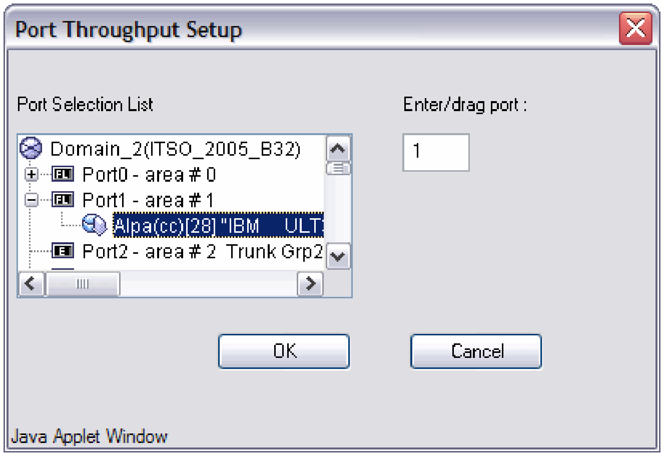
Note: Blade Aggregate Throughput is only available on M12, M14 and SAN256B models.

For each graph, additional options are available by right-clicking the graph.

Example: Port throughput graph

To view the throughput of a port, we select **Performance Graphs** → **Basic Monitoring** → **Port Throughput**. The Port Throughput Setup is then displayed, shown in Figure 1-109. For the SAN256B we have to specify slot and port number. For all other models, we only have to specify the port number.

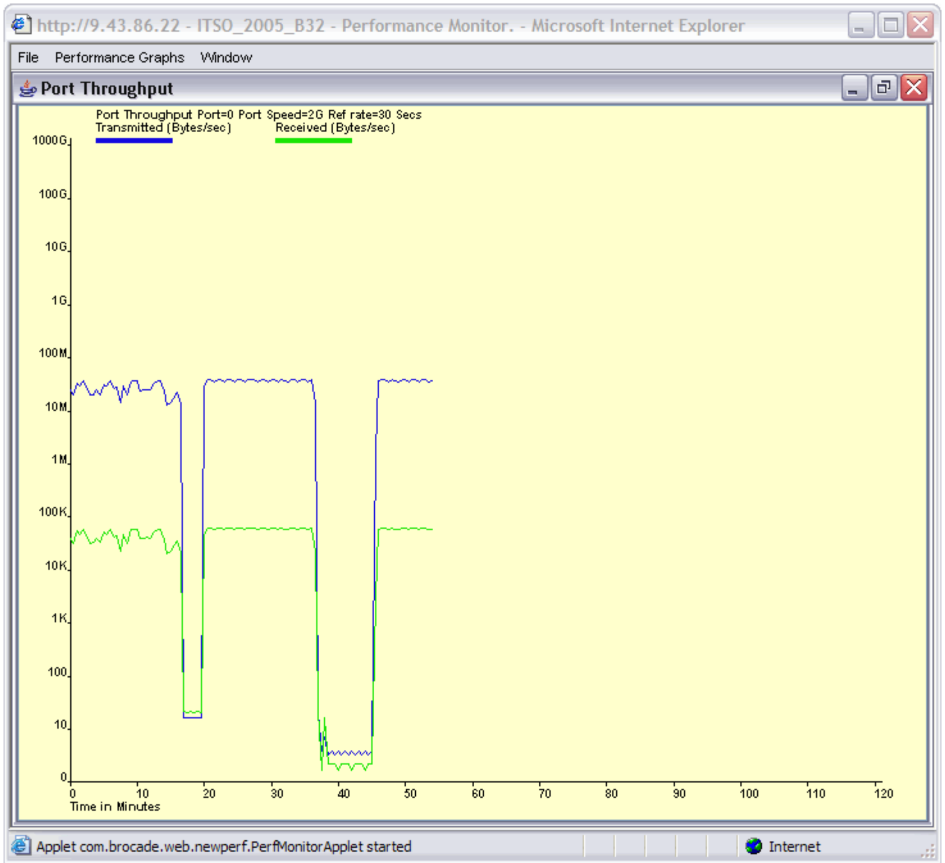
> **Note:** To expand the Domain folder, we have to double-click it to open the port tree.


Port Throughput Setup
Port Selection List
Domain_2(ITSO_2005_B32)
Port0 - area # 0
Port1 - area # 1
Alpa(cc)[28] "IBM ULT
Port2 - area # 2 Trunk Grp2
OK
Cancel
Java Applet Window

Enter/drag port : 1

Figure 1-109 Port throughput graph setup

We enter the number of the slot and port that we want to monitor. A new graph is then added to the canvas. If we zoom in, we get the window shown in Figure 1-110.


http://9.43.86.22 - ITSO_2005_B32 - Performance Monitor. - Microsoft Internet Explorer
File
Performance Graphs
Window
Port Throughput
Port Throughput Port=0 Port Speed=2G Ref rate=30 Secs
Transmitted (Bytes/sec)
Received (Bytes/sec)
1000G
100G
10G
1G
100M
10M
1M
100K
10K
1K
100
10
0
0
10
20
30
40
50
60
70
80
90
100
110
120
Time in Minutes
Internet

Applet com.brocade.web.newperf.PerfMonitorApplet started

Figure 1-110 Port throughput graph

Tip: We can get more detailed information by dragging the mouse pointer over a graph.

Troubleshooting Performance Monitor

When working with the Admin Tool GUI for Performance Monitor, you might experience some difficulty using the drag and drop feature to enter information into the windows. This can be caused by Java issues and results in intermittent behavior whereby the port or other component cannot be dragged or dropped. If you are experiencing these difficulties, we recommend typing in the values.

1.8.16 Advanced Performance Monitoring

Advanced Performance Monitoring is an optionally licensed product that runs on all switch models. It provides SAN performance management through an end-to-end monitoring system that enables you to:

- Increase end-to-end visibility into the fabric
- Enable more accurate reporting for service level agreements and charged access applications
- Improve performance tuning and resource optimization
- Shorten troubleshooting time
- Promote better capacity planning
- Simplify administration and setup
- Increase productivity with pre-formatted and customizable windows and reports

The Performance Monitoring product:

- Monitors transaction performance from its source to its destination
- Provides device performance measurements by port, AL_PA, and LUN
- Reports CRC error measurement statistics
- Measures trunking performance
- Compares IP versus SCSI traffic on each port
- Includes a wide range of predefined reports
- Allows you to create customized user-defined reports

You can administer Performance Monitoring through either Telnet commands or WebTools. If you use WebTools, a WebTools license must also be installed on the switch.

1.8.17 Performance Monitoring with Telnet commands

Three different types of Performance Monitoring can be done using Telnet commands:

- AL_PA monitoring
- End-to-end monitoring
- Filter-based monitoring

AL_PA monitoring

AL_PA monitoring provides information about the number of CRC errors occurring in Fibre Channel frames in a loop configuration. AL_PA monitoring collects CRC error counts for each AL_PA that is attached to a specific port.

End-to-end monitoring

End-to-end monitoring provides information about transaction performance between the transactions source (SID) and destination (DID) on a fabric or a loop. Up to 16 SID-DID pairs per port can be specified. For each of the SID-DID pairs, the following information is available:

- CRC error count on the frames for the SID-DID pair
- Fibre Channel words transmitted from the port for the SID-DID pair
- Fibre Channel words received by the port for the SID-DID pair

Filter-based monitoring

Filter-based monitoring provides information about a filter's hit count. Any parameter in the first 64 bytes of the Fibre Channel frame can be measured. The counter increases each time a frame is filtered through the corresponding port. Examples of port filter statistics that can be measured are:

- SCSI read, write, or read/write commands
- CRC error statistics (port and AL_PA)
- IP versus SCSI traffic comparison

For the latest information on the commands available, refer to the appropriate version of the *Brocade Command Reference Manual*, 53-1000044.

1.8.18 Performance Monitoring with WebTools

You can monitor performance using the WebTools if a WebTools license is also installed. The enhanced Performance Monitoring features in WebTools provide:

- Predefined performance graphs for AL_PA, end-to-end, and filter-based
- User-defined graphs
- Performance canvas for application-level or fabric-level views
- Configuration editor (save, copy, edit, and remove multiple configurations)
- Persistent graphs across restarts (saves parameter data across restarts)
- Print capabilities

Predefined performance graphs

Predefined graphs are provided to simplify performance monitoring and are available from the Performance Graphs → Advanced Monitoring menu. A wide range of end-to-end fabric, LUN, device, and port metrics are included.

Installing Performance Monitoring

To enable Performance Monitoring, you must install a license on each switch that will use this feature. Contact your switch supplier to obtain a license key.

Note: A license might have already been installed on the switch at the factory.

You can install a Performance Monitoring license through Telnet commands or using WebTools. as discussed in “License tab” on page 126 and “Installing a license key through the CLI” on page 134.

1.8.19 Using Advanced Performance Monitoring with WebTools

Attention: As the monitoring of any switch is subjective by nature, we just show the windows to give the reader some familiarity with features that can be monitored.

In Figure 1-111, we can see some of the options that are available.

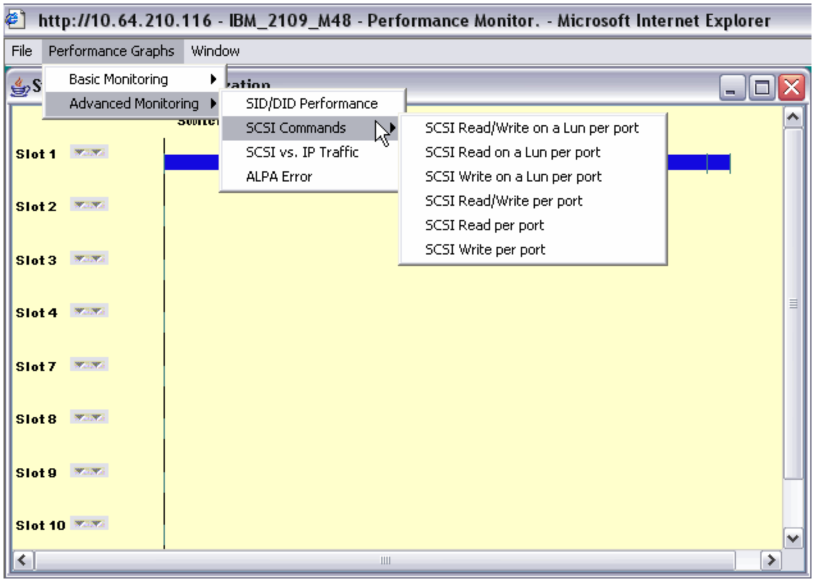

http://10.64.210.116 - IBM_2109_M48 - Performance Monitor. - Microsoft Internet Explorer
File
Performance Graphs
Window
Basic Monitoring
Advanced Monitoring
SID/DID Performance
SCSI Commands
SCSI vs. IP Traffic
ALPA Error
SCSI Read/Write on a Lun per port
SCSI Read on a Lun per port
SCSI Write on a Lun per port
SCSI Read/Write per port
SCSI Read per port
SCSI Write per port
Slot 1
Slot 2
Slot 3
Slot 4
Slot 7
Slot 8
Slot 9
Slot 10

Figure 1-111 Advanced monitor range of options

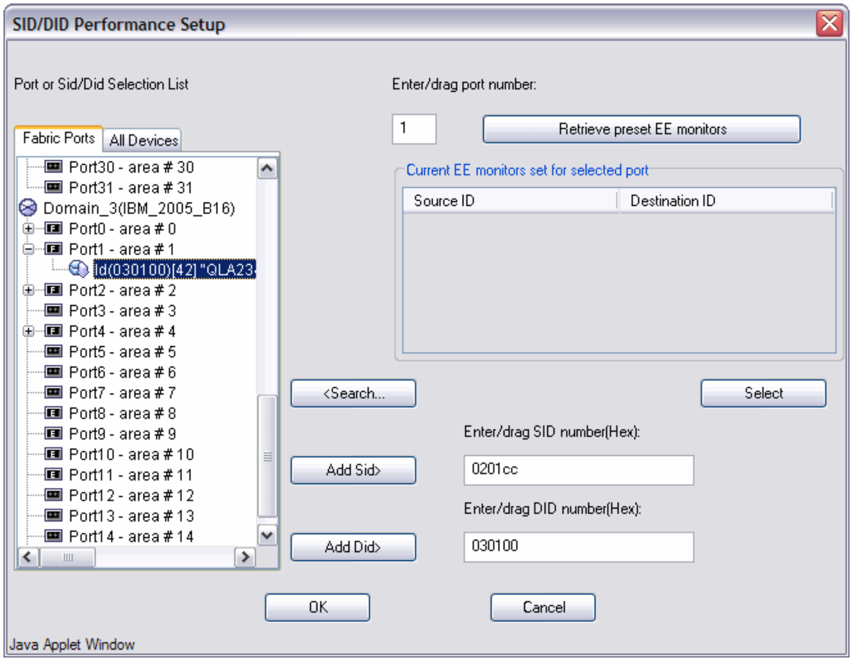
Table 1-21 describes the types of graphs available in the Advanced Monitoring menu.

Table 1-21 Graphs available in Advanced Monitoring feature

Graph name	Type	Description
SID/DID Performance Graph	Line	This graph charts the traffic between a SID (or WWN) and a DID (or WWN) pair on the switch being managed.
SCSI Commands Graph	Line	The total number of Read/Write commands on a given port to a specific LUN. This provides the following choices: SCSI Read/Write on a LUN per port. SCSI Read on a LUN per port. SCSI Write on a LUN per port. SCSI Read/Write per port. SCSI Read per port. SCSI Write per port.
SCSI vs IP Graph	Vertical Bar	Shows percentage of SCSI versus IP frame traffic on each individual port.
AL_PA Error Graph	Line	Displays CRC errors for a given port and a given AL_PA.

SID/DID Performance Graph

Go to **Performance Graphs** → **Advanced Monitoring** → **SID/DID Performance**. To set up the parameters for SID/DID performance monitoring, then use the window shown in Figure 1-112.


SID/DID Performance Setup
Port or Sid/Did Selection List
Fabric Ports
All Devices
Port30 - area # 30
Port31 - area # 31
Domain_3(IBM_2005_B16)
Port0 - area # 0
Port1 - area # 1
id(030100)[42] "QLA23
Port2 - area # 2
Port3 - area # 3
Port4 - area # 4
Port5 - area # 5
Port6 - area # 6
Port7 - area # 7
Port8 - area # 8
Port9 - area # 9
Port10 - area # 10
Port11 - area # 11
Port12 - area # 12
Port13 - area # 13
Port14 - area # 14
Retrieve preset EE monitors
Current EE monitors set for selected port
Source ID
Destination ID
<Search...
Select
Add Sid>
Add Did>
OK
Cancel
Java Applet Window

Enter/drag port number: 1

Enter/drag SID number(Hex): 0201cc

Enter/drag DID number(Hex): 030100

Figure 1-112 SID/DID performance setup

To choose the slot/port and SID/DID that you want to graph:

1. Double-click the Domain you want to work with in the Port Selection List window. A drop-down list of ports appears.
2. Select the port that you want to monitor or change by using one of the following methods:
   a. Type the slot/port number in the window, Enter/drag slot, port number.
   b. Drag the slot/port “folder” from the Slot/Port Selection window to the window, Enter/drag slot, port number.
3. Select the port “folder”, or the small icon that appears next to it. A drop-down list of SID/DID files appears.
4. Select the SID/DID numbers that you want to graph by using one of the following methods:
   a. Type the SID number in the window, Enter/drag SID number(hex). Repeat for the DID number.
   a. Drag the SID “file” from the Port Selection window to the window, Enter/drag SID number(Hex). Repeat for the DID number.
5. Select **OK**.

An example of an SID/DID graph, displaying the traffic between a SID and a DID pair, is shown in Figure 1-113.

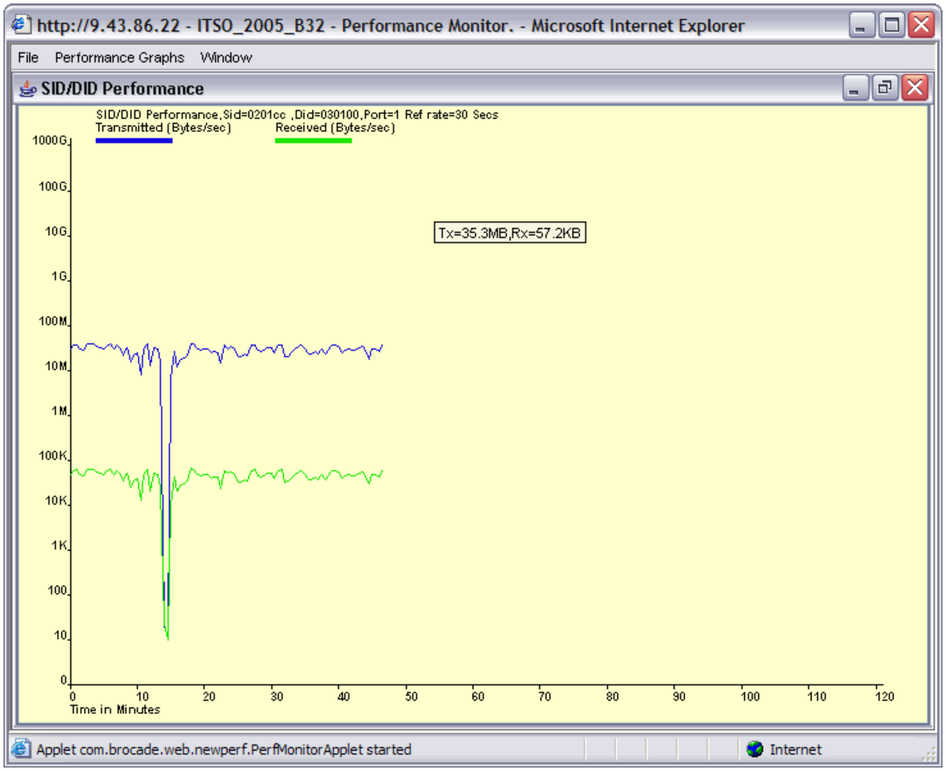

http://9.43.86.22 - ITSO_2005_B32 - Performance Monitor. - Microsoft Internet Explorer
File
Performance Graphs
Window
SID/DID Performance
SID/DID Performance,Sid=0201cc ,Did=030100,Port=1 Ref rate=30 Secs
Transmitted (Bytes/sec)
Received (Bytes/sec)
1000G
100G
10G
1G
100M
10M
1M
100K
10K
1K
100
10
0
Tx=35.3MB,Rx=57.2KB
0
10
20
30
40
50
60
70
80
90
100
110
120
Time in Minutes
Applet com.brocade.web.newperf.PerfMonitorApplet started
Internet

Figure 1-113 SID/DID graph example

Note: SID/DID monitoring monitors traffic on the port logically closest to the SID on the current switch.

Figure 1-114 shows several switches and the proper ports on which to add performance monitors for a specified SID/DID pair.

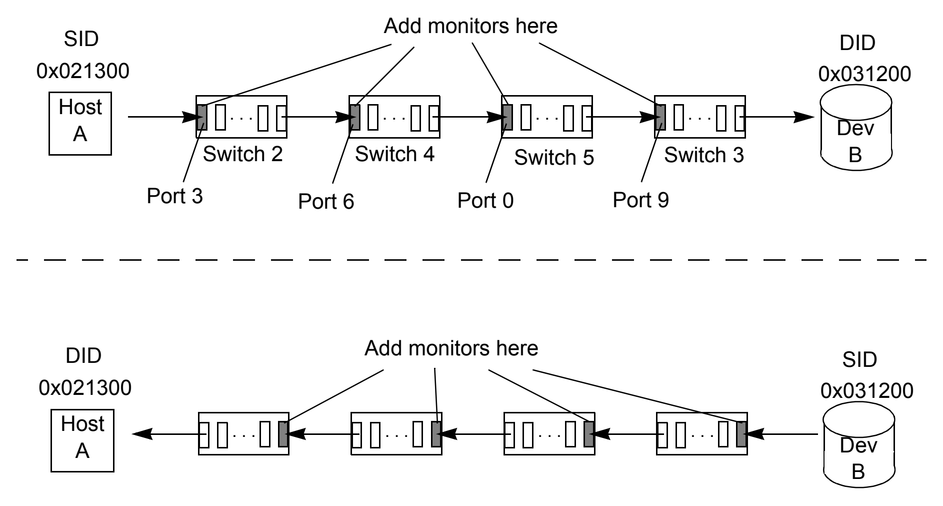

SID
0x021300
Host A
Add monitors here
DID
0x031200
Switch 2
Switch 4
Switch 5
Switch 3
Dev B
Port 3
Port 6
Port 0
Port 9
DID
0x021300
Host A
Add monitors here
SID
0x031200
Dev B

Figure 1-114 Proper placement of SID/DID performance monitors

In Figure 1-114, monitoring Port 6 on Switch 4, specifying Host A as the SID and Dev B as the DID is correct.

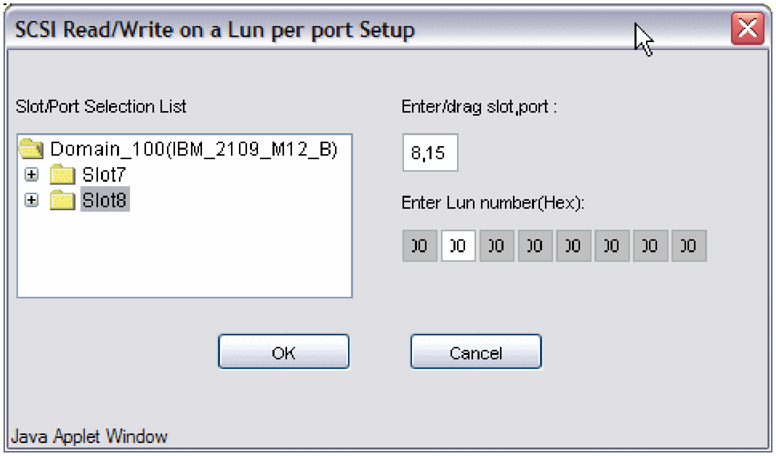
But monitoring Port 6 on Switch 4, specifying Dev B as the SID and Host A as the DID, does not display a valid graph, because traffic is shown as null.

SCSI command graph

When you select the SCSI graph in **Performance Graphs** → **Advanced Monitoring** → **SCSI Commands**, the following options are displayed in a pull-down menu:

- SCSI Read/Write on a LUN per port
- SCSI Read on a LUN per port
- SCSI Write on a LUN per port
- SCSI Read/Write per port
- SCSI Read per port
- SCSI Write per port

Each graph prompts you with a data entry window to select the port and LUN to be monitored, as shown in Figure 1-115. In this example, we want to monitor **SCSI Read** and Write commands on LUN 0 going through slot 8, port 15 of the current switch.


SCSI Read/Write on a Lun per port Setup
Slot/Port Selection List
Domain_100(IBM_2109_M12_B)
Slot7
Slot8
OK
Cancel
Java Applet Window

Enter/drag slot,port : 8,15

Enter Lun number(Hex): 00 00 00 00 00 00 00 00

Figure 1-115 SCSI read/write LUN per port setup

To select the port and LUN to monitor:

1. Double-click the folder in the Slot/Port Selection List window. A drop-down list of ports appears.
2. Select the port that you want to monitor or change by using one of the following methods:
    a. Type the port number in the window, Enter/drag slot, port number.
    b. Drag the slot/port “file” from the Slot/Port Selection window to the window, Enter/drag slot, port number.
3. Enter a LUN number in the window, Enter LUN Number (Hex).

    You can enter only four LUN numbers at a time.
4. Select **OK**.

A graph displaying the total number of Read and/or Write commands on a given port to a specific LUN is displayed.

An example of a SCSI graph, using the Write on a LUN per port option, is shown in Figure 1-116.

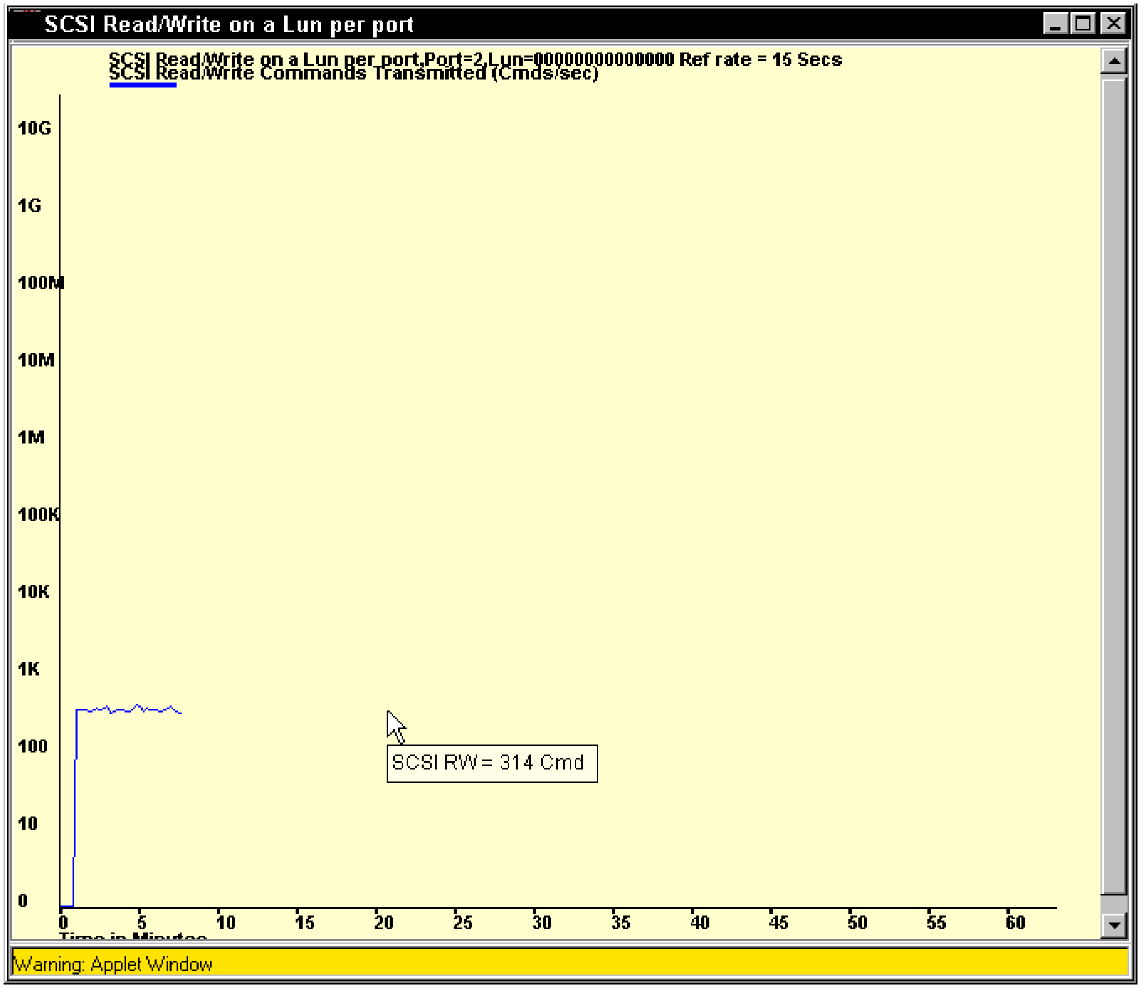

SCSI Read/Write on a Lun per port
SCSI Read/Write on a Lun per port,Port=2,Lun=0000000000000000 Ref rate = 15 Secs
SCSI Read/Write Commands Transmitted (Cmds/sec)
10G
1G
100M
10M
1M
100K
10K
1K
100
10
0
0
5
10
15
20
25
30
35
40
45
50
55
60
SCSI RW = 314 Cmd
Warning: Applet Window

Figure 1-116 SCSI Read/Write on a LUN per port graph

SCSI versus IP Traffic graph

The SCSI versus IP Traffic graph is accessible via **Performance Graphs** → **Advanced Monitoring** → **SCSI versus IP Traffic**.

An example of this graph, displaying the percentage of SCSI versus IP frame traffic, is shown in Figure 1-117.

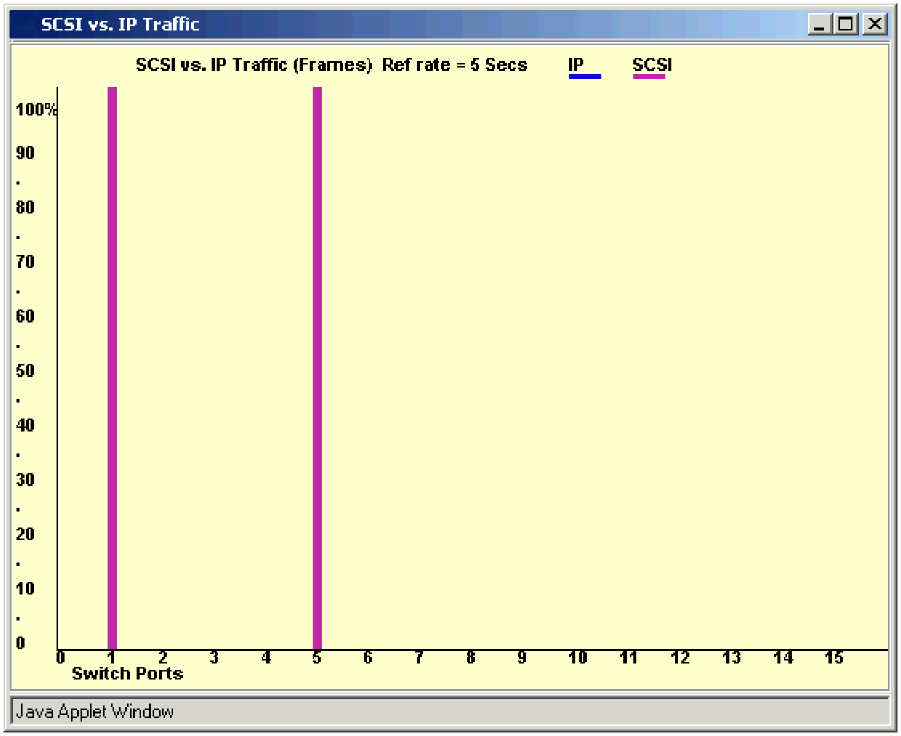

SCSI vs. IP Traffic
SCSI vs. IP Traffic (Frames) Ref rate = 5 Secs
IP
SCSI
100%
90
80
70
60
50
40
30
20
10
0
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Switch Ports
Java Applet Window

Figure 1-117 SCSI versus IP traffic graph

This graph gives us the percentage of IP and SCSI traffic on the current switch on a port basis.

AL_PA Error graph

This feature is only available on the older switches based upon the Bloom ASIC and as such, we do not cover it here.

1.8.20 Using Advanced Performance Monitoring with the CLI

Three different types of Performance Monitoring can be done using Telnet commands:

- AL_PA monitoring
- End-to-end monitoring
- Filter-based monitoring

AL_PA monitoring

This feature is only available on the older switches based upon the Bloom ASIC and as such is not detailed here.

Adding end-to-end monitors

Use the **`perfAddEEMonitor`** command to add an end-to-end monitor to a port. With this command we specify the port, the SID, and the DID that we want to monitor. Depending on the application, we can select any port along the routing path for monitoring.

Figure 1-118 shows two devices: Host A, which is connected to port 3 on switch 2; and Dev B, which is connected to port 2 on switch 3.

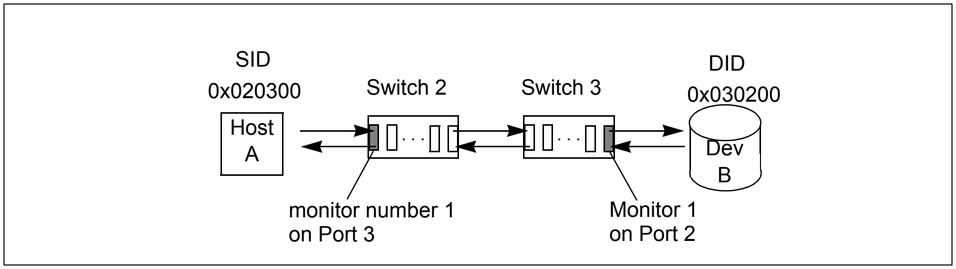


Figure 1-118 Setting end-to-end monitor on a port

To monitor the traffic from Host A to Dev B, work on Switch 2 and add a monitor to port 3, specifying 0x020300 as the SID and 0x030200 as the DID. To monitor the traffic from Dev B to Host A, work on Switch 3 and add a monitor to port 2, specifying 0x030200 as the SID and 0x020300 as the DID.

We use **`perfAddEEMonitor`** as shown in Example 1-15.

Example 1-15 Add an end-to-end monitor to switch 1 port 7

```
IBM_2005_B32:admin>  perfAddEEMonitor 3 0x020300 0x030200
End-to-End monitor number 0 added.
```

As shown in Example 1-15, monitor number 0 counts the frames that have an SID of 0x020300 and a DID of 0x030200. For monitor number 0, RX_COUNT is the number of words from Host A to Dev B, CRC_COUNT is the number of frames from Host A to Dev B with CRC errors, and TX_COUNT is the number of words from Dev B to Host A.

Attention: The monitor must be properly placed.

In Figure 1-118, if we add a monitor to switch2, port 3, specifying Dev B as the SID and Host A as the DID, no counters are incremented:

- Valid: `perfAddEEMonitor 3,"0x020300","0x030200"`
- Not valid: `perfAddEEMonitor 3,"0x030200","0x020300"`

Setting a mask for end-to-end monitors

End-to-end monitors count the number of words in Fibre Channel frames that match a specific SID/DID pair. If we want to match only part of the SID or DID, we can set a mask on the port to compare only certain parts of the SID or DID. With no mask set, the frame must match the entire SID and DID to trigger the monitor. By setting a mask, we can choose to have the frame match only one or two of the three fields (Domain ID, Area ID, AL_PA) to trigger the monitor.

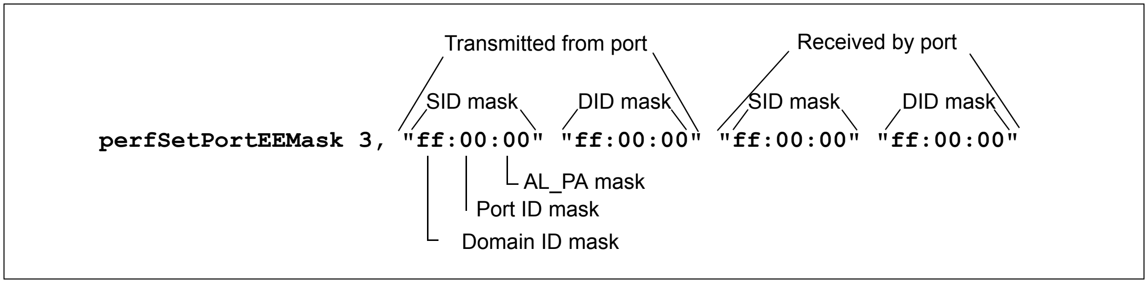
> **Note:** We can set only one mask per port. The mask is applied to all of the end-to-end monitors on a port. If we subsequently create new monitors on the port, the mask is applied to these new monitors as well. All of the counters are reset when we set the mask.

The mask is specified in the form “dd:aa:pp” where dd is the domain ID mask, aa is the Port ID mask, and pp is the AL_PA mask. The values for dd, aa, and pp are either:

- `ff` (the field must match)
- `00` (the field is ignored).

Use the **`perfSetPortEEMask`** to set a mask for end-to-end monitors. The command sets the mask for all end-to-end monitors of a port.

The **`perfSetPortEEMask command`** sets a mask for the domain ID, Port ID, and AL_PA of the SIDs and DIDs for frames transmitted from and received by the port. Figure 1-119 shows the mask positions in the command.



```
perfSetPortEEMask 3, "ff:00:00" "ff:00:00" "ff:00:00" "ff:00:00"
```

Figure 1-119 Mask positions for end-to-end monitors

In Figure 1-119, a mask ("ff") is set on port 3 to compare the domain ID fields on the SID and DID in all frames (transmitted and received) on port 3. The AL_PA and Port ID fields in all frames are ignored, as no mask is set on these fields.

If you set the following monitor on port 3:

```
perfAddEEMonitor 3,"0x020300","0x030200"
```

Then, without any mask, then the SID must be `0x020300` and the DID must be `0x030200` to trigger the monitor.

If you set the mask shown in Figure 1-119, then the frame SID and DID must match only the domain ID portion of the specified SID-DID pair. That is, frames with SID of "0x02nnnn" and DID of "0x03nnnn" trigger the monitor, where nnnn is any number.

Each port can have only one EE mask. The mask is applied to all end-to-end monitors on the port. You cannot specify individual masks for each monitor on the port. If you define a new end-to-end monitor on a port after you have created a mask for that port, the mask is automatically applied to the new monitor.

The default EE mask value upon power-on is "ff:ff:ff" for everything — SID and DID on all transmitted and received frames.

In Example 1-16, we use the **`perfSetPortEEMask command`** to set a mask on the SID and DID domain ID of frames transmitted from switch 2, port 3. After the mask is set, the monitor number created previously counts the number of words in the incoming Fibre Channel frames that have an SID of 0x02nnnn and a DID of 0x03nnnn, where nnnn is any number.

Example 1-16 Set a mask on switch2, port 3

```
IBM_2005_B32:admin>  perfAddEEMonitor 3 0x020300 0x030200
End-to-End monitor number 1 added.
IBM_2005_B32:admin> perfSetPortEEMask 3 “00:00:00” “00:00:00” “ff:00:00”
“ff:00:00”
Changing EE mask for this pport will cause ALL EE monitors on this port to be
deleted.
continue? (yes, y, no, n): [no] y
The EE mask on port 3 is set and EE Monitors on this port are deleted.
IBM_2005_B32:admin>
```

Displaying the end-to-end mask of a port

You can use the **`perfShowPortEEMask`** command to display the current end-to-end mask of a port as shown in Example 1-17.

Example 1-17 Displaying the end-to-end port mask

```
IBM_2005_B32:admin> perfShowPortEEMask 3
The EE mask on port 3 is set by application NONE.

TxSID Domain:  off
TxSID Area:    off
TxSID ALPA:    off
TxDID Domain:  off
TxDID Area:    off
TxDID ALPA:    off
RxSID Domain:  on
RxSID Area:    off
RxSID ALPA:    off
RxDID Domain:  on
RxDID Area:    off
RxDID ALPA:    off
```

The end-to-end mask has 12 fields, with each having a value of `on` or `off`.

Displaying the end-to-end monitors

We use the **`perfShowEEMonitor`** command to display the end-to-end monitors defined on the port. We can display cumulative counters as shown in Example 1-18.

Example 1-18 Displaying end-to-end monitor using perfShowEEMonitor

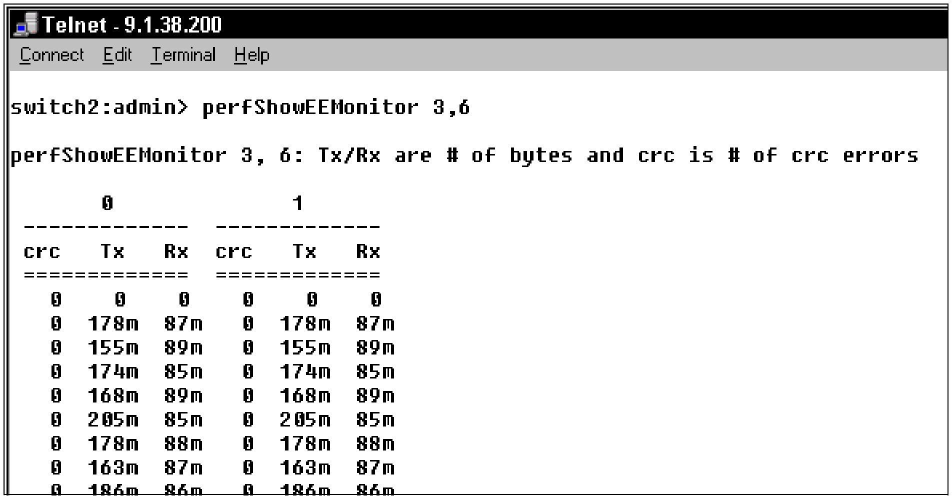
```
ITSO_2005_B32:admin> perfShowEEMonitor 3

There are 1 end-to-end monitor(s) defined on port      3.

KEY     SID     DID     OWNER_APP    OWNER_IP_ADDR        TX_COUNT            RX_COUNT
--------------------------------------------------------------------------------------
 0  0x030200  0x20300   WEB_TOOLS     9.43.32.109        0x000000000000184c  0x0000000000002fb0
```

This command displays:

- `Key`: Monitor number
- `SID`: Source ID
- `DID`: Destination ID
- `OWNER_APP`: TELNET or WEB_TOOLS
- `OWNER_IP_ADDR`: IP address of the owner of the filter monitor
- `TX_COUNT`: Transmitting frame count
- `RX_COUNT`: Receiving frame count
- `CRC_COUNT`: CRC error count

The cumulative counters are 64-bit values in hexadecimal format.

If we specify an interval number in the **`perfShowEEMonitor`** command, the command displays a rolling table of CRC error, Tx, and Rx counters on a per-interval basis for all the valid monitors on the port as shown in Figure 1-120. The counter values are the number of bytes, in decimal format.



```
switch2:admin> perfShowEEMonitor 3,6

perfShowEEMonitor 3, 6: Tx/Rx are # of bytes and crc is # of crc errors

       0              1
 -------------  -------------
 crc   Tx   Rx  crc   Tx   Rx
 =============  =============
   0    0    0    0    0    0
   0  178m  87m   0  178m  87m
   0  155m  89m   0  155m  89m
   0  174m  85m   0  174m  85m
   0  168m  89m   0  168m  89m
   0  205m  85m   0  205m  85m
   0  178m  88m   0  178m  88m
   0  163m  87m   0  163m  87m
   0  186m  86m   0  186m  86m
```

Figure 1-120 Displaying end-to-end monitor with a interval

The counter values in Figure 1-120 are the number of bytes in decimal format. The “m” stands for megabytes. You might also see “g” which stands for gigabytes, or “k” which stands for kilobytes.

Not all platforms support the counting of CRC errors. As such, you might only see the Tx and Rx columns displayed.

Note: The minimum interval value that can be specified is 5 seconds.

Deleting end-to-end monitors

Use the **`perfDelEEMonitor`** command to delete an end-to-end monitor on a port as shown in Example 1-19. Indicate which monitor to delete by specifying the monitor number that was returned by a previous **`perfAddEEMonitor`** command.

Example 1-19 Deleting end-to-end monitors

```
ITSO_2005_B32:admin> perfDelEEMonitor 3 0
End-to-End monitor number 0 deleted
```

The following command deletes all of the end-to-end monitors on port 2:

```
sw1:admin> perfDelEEMonitor 2
This will remove ALL EE monitors on port 2, continue? [y|n]y
```

Clearing end-to-end monitor counters

To clear all of the end-to-end monitor counters on a port, use the **`perfSetPortEEMask command`** to reset all of the end-to-end monitor counters on that port.

The **`perfSetPortEEMask`** command also sets the end-to-end mask, so if you do not want to change the mask, you must re-specify the current mask settings. You can view the current mask settings using the **`perfShowPortEEMask`** command.

To clear the counters for a single end-to-end monitor, delete the monitor using the **`perfDelEEMonitor`** command, and then add the monitor again, using the **`perfAddEEMonitor`** command.

Filter-based monitoring

Filter-based monitoring provides information about a filter's hit count. Any parameter in the first 64 bytes of the Fibre Channel frame can be measured. The counter increases each time a frame is filtered through the corresponding port. Examples of port filter statistics that can be measured are:

- SCSI read, write, or read/write commands
- CRC error statistics (port and AL_PA)
- IP versus SCSI traffic comparison

The filter can be a standard filter (for example, a read command filter that counts the number of read commands that have been received by the port) or a user-defined filter that you customize for your particular use.

The maximum number of filters is eight per port, in any combination of standard filters and user-defined filters.

Adding standard filter-based monitors

This section describes how to add standard filter-based monitors to a port. Use the telnet commands listed in Table 1-22 to define filter-based monitors on a port.

Table 1-22 Add filter-based monitor commands

Command	Description
perfAddReadMonitor	Count the number of SCSI Read commands
perfAddWriteMonitor	Count the number of SCSI Write commands
perfAddRWMonitor	Count the number of SCSI Read and Write commands
perfAddSCSIMonitor	Count the number of SCSI traffic frames
perfAddIPMonitor	Count the number of IP traffic frames

In Example 1-20 we add several filter monitors to switch2, port 3.

Example 1-20 Adding filter monitors to a port

```
ITSO_2005_B32:admin> perfAddWriteMonitor 3
SCSI Write filter monitor #1 added
ITSO_2005_B32:admin> perfAddSCSIMonitor 3
SCSI traffic frame monitor #2 added
ITSO_2005_B32:admin> perfAddIPMonitor 3
IP traffic frame monitor #3 added

ITSO_2005_B32:admin> perfShowFilterMonitor 3

There are 4 filter-based monitors defined on port 3.

KEY   ALIAS   OWNER_APP         OWNER_IP_ADDR     FRAME_COUNT
-------------------------------------------------------------------
 0  SCSI Read  TELNET                N/A        0x0000000000000000
 1  SCSI Write TELNET                N/A        0x0000000000000000
 2  SCSI Frame TELNET                N/A        0x0000000000000028
 3  IP Frame   TELNET                N/A        0x0000000000000000
```

Adding user-defined filter-based monitors

In addition to the standard filters (read, write, read/write, and frame count), you can create custom filters to qualify frames for statistics gathering to fit your own special requirements.

To define a custom filter, use the **`perfAddUserMonitor`** telnet command. You must specify a series of offsets, masks, values and an alias for the monitor. The following actions are performed. For all incoming frames, the switch:

1. Locates the byte found in the frame at the specified offset
2. Applies the mask to the byte found in the frame
3. Compares the value with the given values in the **`perfAddUserMonitor`** command
4. Increments the filter counter if a match is found

You can specify up to six different offsets for each port, and up to four values to compare against each offset.

If more than one offset is required to properly define a filter, the bytes found at each offset must match one of the given values for the filter to increment its counter. If one or more of the given offsets does not match any of the given values, the counter does not increment.

The value of the offset must be between 0 and 63, in decimal format. Byte 0 indicates the first byte of the Start of Frame (SOF), byte 4 is the first byte of the frame header, and byte 28 is the first byte of the payload. Thus only the SOF, frame header, and first 36 bytes of payload can be selected as part of a filter definition.

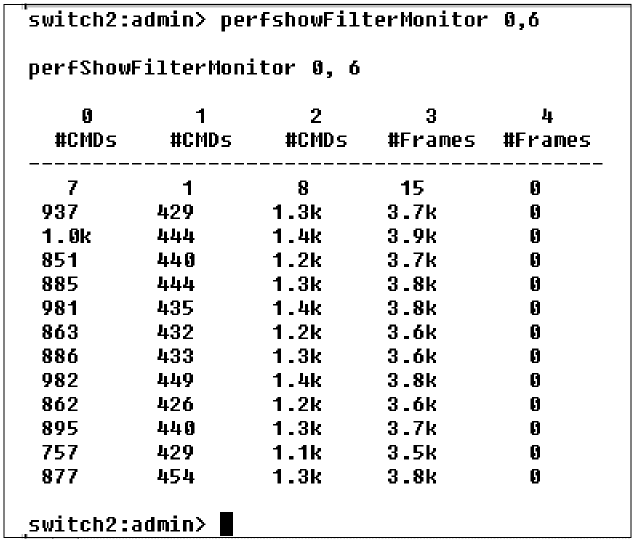
Displaying filter-based monitors

Use the **`perfShowFilterMonitor`** command to display all the filter-based monitors of a port. You can display a cumulative count of the traffic detected by the monitors, or you can display a snapshot of the traffic at specified intervals.

> **Note:** Intervals must be specified in multiples of 5 seconds, for example, 5, 10, 15, 20, 25, etc., because registers are scanned every 5 seconds.

This command displays all the filter-based monitors defined on the specified port. It displays all the valid monitor numbers and user-defined aliases on the specified port.

Figure 1-121 shows the traffic at a specified interval of six seconds on port 0.



```
switch2:admin> perfshowFilterMonitor 0,6

perfShowFilterMonitor  0, 6

    0        1        2        3        4
  #CMDs    #CMDs    #CMDs   #Frames  #Frames
--------------------------------------------
   7        1        8       15        0
 937      429      1.3k     3.7k       0
 1.0k     444      1.4k     3.9k       0
 851      440      1.2k     3.7k       0
 885      444      1.3k     3.8k       0
 981      435      1.4k     3.8k       0
 863      432      1.2k     3.6k       0
 886      433      1.3k     3.6k       0
 982      449      1.4k     3.8k       0
 862      426      1.2k     3.6k       0
 895      440      1.3k     3.7k       0
 757      429      1.1k     3.5k       0
 877      454      1.3k     3.8k       0

switch2:admin> █
```

Figure 1-121 Displaying filter monitor

> **Note:** A defined filter will only increment if set on receiving ports.

Deleting filter-based monitors

To delete a filter-based monitor, first list the valid monitor numbers using the **`perfShowFilterMonitor`** command, then use the **`perfDelFilterMonitor`** command to delete a specific monitor. If you do not specify which monitor number to delete, you are asked if you want to delete all entries.

1.8.21 Fabric Watch button

To access the Fabric Watch function, click the “magnifying glass” button (labeled **Watch**) from the Switch View, as shown in Figure 1-122.

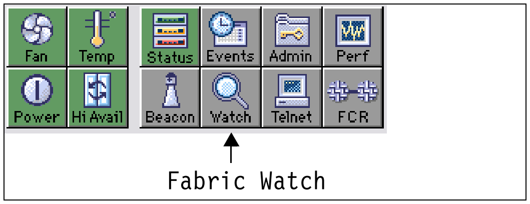
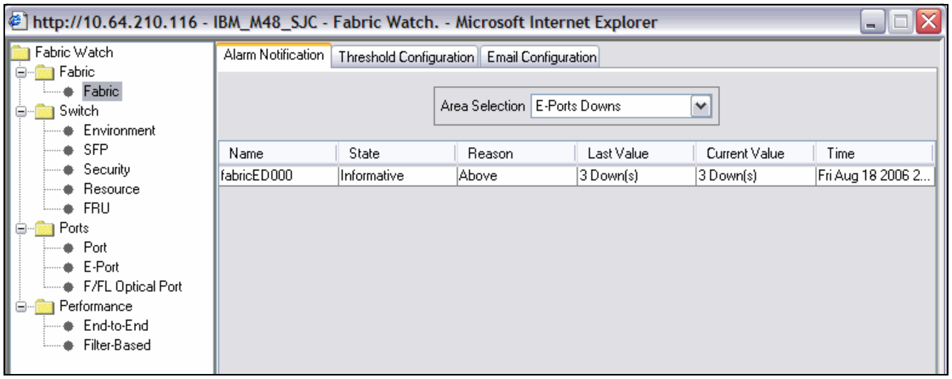

Fan
Temp
Status
Events
Admin
Perf
Power
Hi Avail
Beacon
Watch
Telnet
FCR
Fabric Watch

Figure 1-122 Fabric watch button

Accessing Fabric Watch requires an admin logon and password. When authentication is complete, the Fabric Watch window is then displayed, as shown in Figure 1-123.


http://10.64.210.116 - IBM_M48_SJC - Fabric Watch. - Microsoft Internet Explorer
Fabric Watch
Fabric
Fabric
Switch
Environment
SFP
Security
Resource
FRU
Ports
Port
E-Port
F/FL Optical Port
Performance
End-to-End
Filter-Based
Alarm Notification
Threshold Configuration
Email Configuration

Area Selection: E-Ports Downs

Name	State	Reason	Last Value	Current Value	Time
fabricED000	Informative	Above	3 Down(s)	3 Down(s)	Fri Aug 18 2006 2...

Figure 1-123 Fabric watch initial view

The window is divided into two sections. The left-hand side has a tree structure that lists the *Classes* that can be monitored using Fabric Watch. If you expand the *Classes*, all the *Areas* that are associated with a particular *Class* are displayed.

The main part of the window on the right-hand side has a display with three tabs:

- Alarm Notification tab
- Threshold Configuration tab
- Email Configuration tab

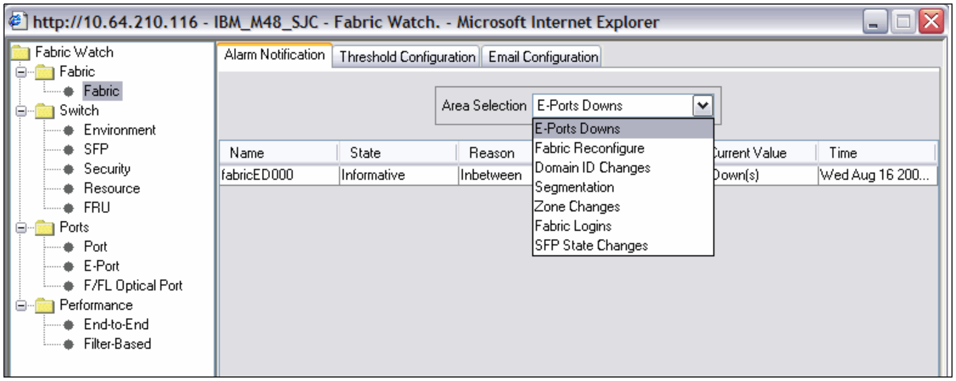
Alarm Notification

Use the **Alarm Notification** tab to view the information for all elements of the Fabric Watch, Fabric, or Performance Monitor classes. The information displayed includes:

- The name of the fabric
- The current value
- The last event type
- The last event time
- The last event value
- The last event state

The Alarm Notification refreshes the displayed information according to the threshold configuration.

The **Alarm Notification** tab is shown in Figure 1-124.


http://10.64.210.116 - IBM_M48_SJC - Fabric Watch. - Microsoft Internet Explorer
Fabric Watch
Fabric
Fabric
Switch
Environment
SFP
Security
Resource
FRU
Ports
Port
E-Port
F/FL Optical Port
Performance
End-to-End
Filter-Based
Alarm Notification
Threshold Configuration
Email Configuration
E-Ports Downs
Fabric Reconfigure
Domain ID Changes
Segmentation
Zone Changes
Fabric Logins
SFP State Changes

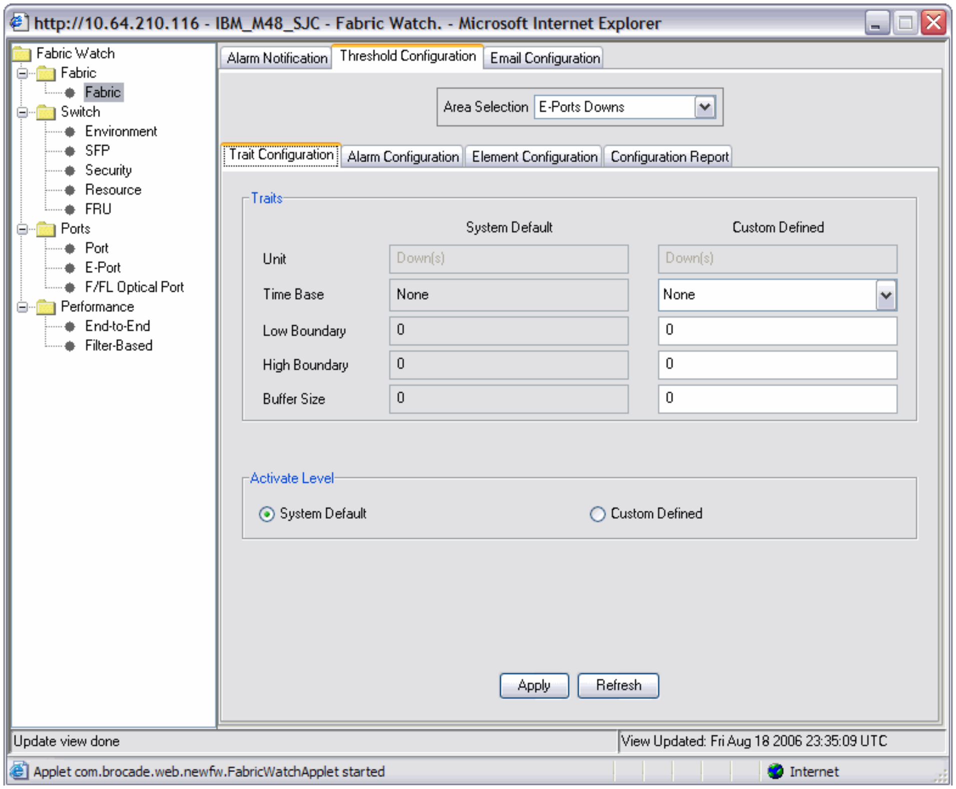
Area Selection: E-Ports Downs

Name	State	Reason	urrent Value	Time
fabricED000	Informative	Inbetween	own(s)	Wed Aug 16 200...

Figure 1-124 Fabric watch alarm notifications

Configuring thresholds

Use the **Thresholds Configuration** tab to view and configure Fabric Watch thresholds for the Fabric Watch class currently selected in the organizational tree on the left side of the window. The **Thresholds Configuration** tab is shown in Figure 1-125.


http://10.64.210.116 - IBM_M48_SJC - Fabric Watch. - Microsoft Internet Explorer
Fabric Watch
Fabric
Fabric
Switch
Environment
SFP
Security
Resource
FRU
Ports
Port
E-Port
F/FL Optical Port
Performance
End-to-End
Filter-Based
Alarm Notification
Threshold Configuration
Email Configuration
Trait Configuration
Alarm Configuration
Element Configuration
Configuration Report
Traits
Activate Level
Apply
Refresh
Internet

Area Selection: E-Ports Downs

	System Default	Custom Defined
Unit	Down(s)	Down(s)
Time Base	None	None
Low Boundary	0	0
High Boundary	0	0
Buffer Size	0	0

Activate Level: ● System Default ○ Custom Defined

Update view done

View Updated: Fri Aug 18 2006 23:35:09 UTC

Applet com.brocade.web.newfw.FabricWatchApplet started

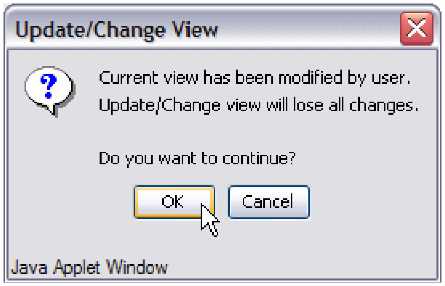
Figure 1-125 Configure Thresholds

The Thresholds Configuration display changes according to the Class and Area selected in the organizational tree. However, the **Thresholds Configuration** tab always contains the same buttons, as follows:

- **Default:** Click to return settings to default values.
- **Custom Define:** Specify new settings.
- **Apply:** Click to apply the values specified in the current display.
- **Refresh:** Refresh view with current information from switch.

> **Important:** When making changes in a given window, they are not saved until we click the **Apply** button.

If we do not want to save the changes that we made, we can cancel them by clicking another tab to view. Doing this brings up the *Update/Change View* warning window shown in Figure 1-126, where we are able to click **Yes** and continue without saving the changes.


Update/Change View
OK
Cancel
Java Applet Window

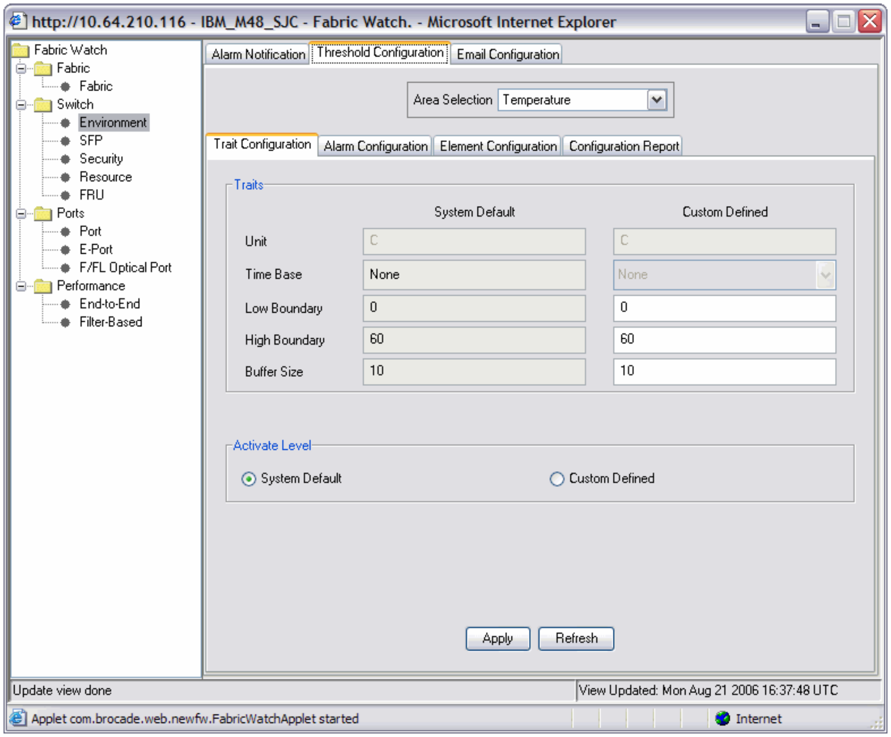
Current view has been modified by user.
Update/Change view will lose all changes.

Do you want to continue?

Figure 1-126 Update/Change view warning

Thresholds for the Environmental classes

The Environmental classes are displayed by highlighting *Environment* in the panel on the left and then clicking the **Threshold Configuration** tab as shown in Example 1-127.


http://10.64.210.116 - IBM_M48_SJC - Fabric Watch. - Microsoft Internet Explorer
Fabric Watch
Fabric
Fabric
Switch
Environment
SFP
Security
Resource
FRU
Ports
Port
E-Port
F/FL Optical Port
Performance
End-to-End
Filter-Based
Alarm Notification
Threshold Configuration
Email Configuration
Trait Configuration
Alarm Configuration
Element Configuration
Configuration Report
Traits
Activate Level
Apply
Refresh
Internet

Area Selection: Temperature

	System Default	Custom Defined
Unit	C	C
Time Base	None	None
Low Boundary	0	0
High Boundary	60	60
Buffer Size	10	10

Activate Level: ● System Default ○ Custom Defined

Update view done

View Updated: Mon Aug 21 2006 16:37:48 UTC

Applet com.brocade.web.newfw.FabricWatchApplet started

Figure 1-127 Environmental Thresholds

The panel contains four tabs to define how we intend to monitor the environmental factors of the switch. They are: *Trait Configuration, Alarm Configuration, Element Configuration,* and *Configuration Report.*

Each tab contains an Area Selection pulldown menu to select the Fabric Watch area. In the example in Table 1-23, we selected Temperature.

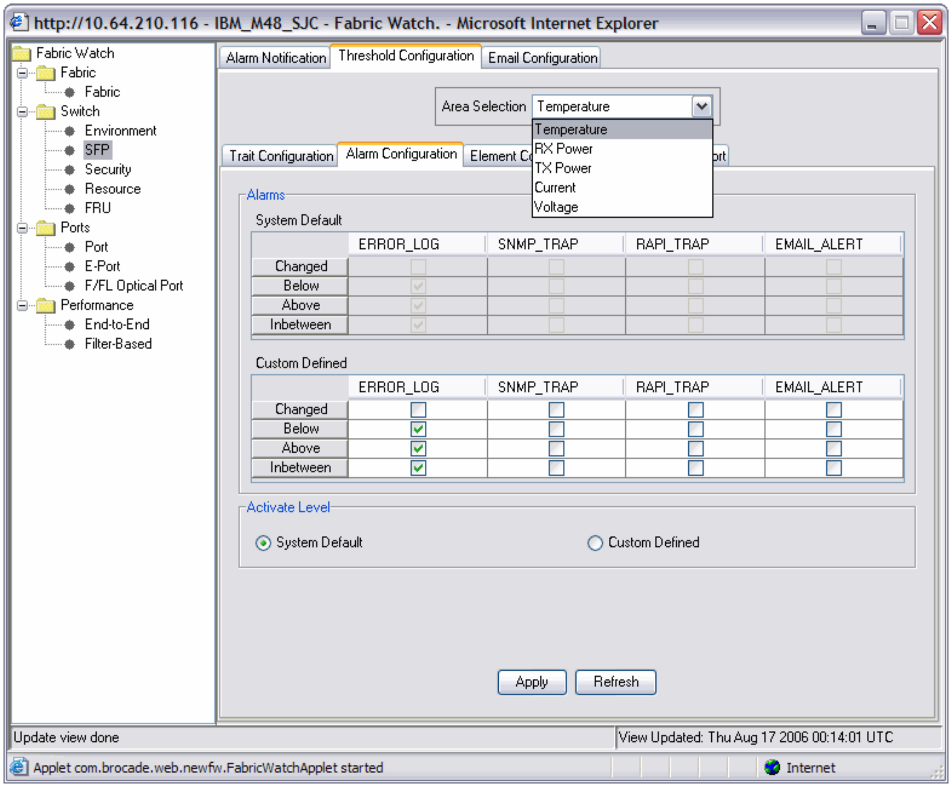
The values and information on the **Trait Configuration** tab are described in Table 1-23.

Table 1-23 Trait configuration threshold

Value	Description
Unit	The string used to define the unit of measurement for the area
Time base	The time base for the area
Low Boundary	The low threshold for the event setting comparison
High Boundary	The high threshold for the event setting comparison
Buffer size	Size of the buffer zone in the event setting comparison
Activate level	Radio button to use Default settings or Custom Define settings
Apply	Apply the new values to the switch
Refresh	Refresh view with current information from the switch

Thresholds for the SFP Classes

The SFP classes are displayed by highlighting SFP in the panel on the left and clicking the **Alarm Notification** tab. The *Area Selection* pull-down menu displays the Classes to be configured as shown in Figure 1-128 on page 186.


http://10.64.210.116 - IBM_M48_SJC - Fabric Watch. - Microsoft Internet Explorer
Fabric Watch
Fabric
Fabric
Switch
Environment
SFP
Security
Resource
FRU
Ports
Port
E-Port
F/FL Optical Port
Performance
End-to-End
Filter-Based
Alarm Notification
Threshold Configuration
Email Configuration
Area Selection
Temperature
Temperature
RX Power
TX Power
Current
Voltage
Trait Configuration
Alarm Configuration
Element C
Alarms
Activate Level
Apply
Refresh
Internet

System Default

	ERROR_LOG	SNMP_TRAP	RAPI_TRAP	EMAIL_ALERT
Changed	☐	☐	☐	☐
Below	☑	☐	☐	☐
Above	☑	☐	☐	☐
Inbetween	☑	☐	☐	☐

Custom Defined

	ERROR_LOG	SNMP_TRAP	RAPI_TRAP	EMAIL_ALERT
Changed	☐	☐	☐	☐
Below	☑	☐	☐	☐
Above	☑	☐	☐	☐
Inbetween	☑	☐	☐	☐

● System Default ○ Custom Defined

Update view done

View Updated: Thu Aug 17 2006 00:14:01 UTC

Applet com.brocade.web.newfw.FabricWatchApplet started

Figure 1-128 SFP thresholds

The available areas are Temperature, RX Power, TX Power, Current and Voltage. The **Alarm Configuration** tab has two areas to show the Default settings and the Customer define settings. These areas are described in Table 1-24.

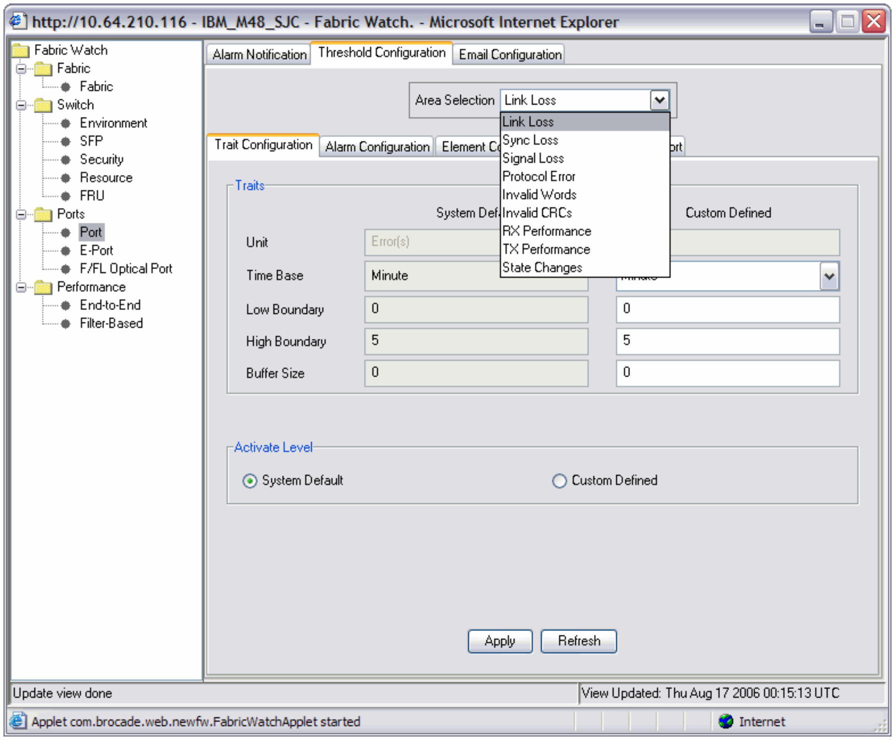
Table 1-24 Alarm Configuration settings

Value	Description
Changed	Event of counter changed
Below	Event of counter fell below low boundary
Above	Event of counter fell above high boundary
Inbetween	Event of counter is between the high/low boundaries
ERROR_LOG	Event notification to error log
SNMP_TRAP	Event notification through SNMP trap
RAPI_TRAP	Event notification through RAPI trap

Value	Description
EMAIL_ALERT	Event notification through e-mail
System Default	Radio button indicating system defaults taken
Custom Define	Radio button indicating custom defined

Thresholds for the remaining classes

The Port, E_Port, F/FL Copper Port, F/FL Optical Port classes display the following fields for each area (Link Loss, Sync Loss, Signal Loss, Protocol Error, Invalid Words, Invalid CRCs, RX Performance, TX Performance, State Changes. The thresholds for the Port class are displayed as shown in Figure 1-129.


http://10.64.210.116 - IBM_M48_SJC - Fabric Watch. - Microsoft Internet Explorer
Fabric Watch
Fabric
Fabric
Switch
Environment
SFP
Security
Resource
FRU
Ports
Port
E-Port
F/FL Optical Port
Performance
End-to-End
Filter-Based
Alarm Notification
Threshold Configuration
Email Configuration
Link Loss
Sync Loss
Signal Loss
Protocol Error
Invalid Words
Invalid CRCs
RX Performance
TX Performance
State Changes
Trait Configuration
Alarm Configuration
Element C
Traits
Activate Level
Apply
Refresh
Internet

Area Selection: Link Loss

	System Def	Custom Defined
Unit	Error(s)	
Time Base	Minute	
Low Boundary	0	0
High Boundary	5	5
Buffer Size	0	0

● System Default ○ Custom Defined

Update view done

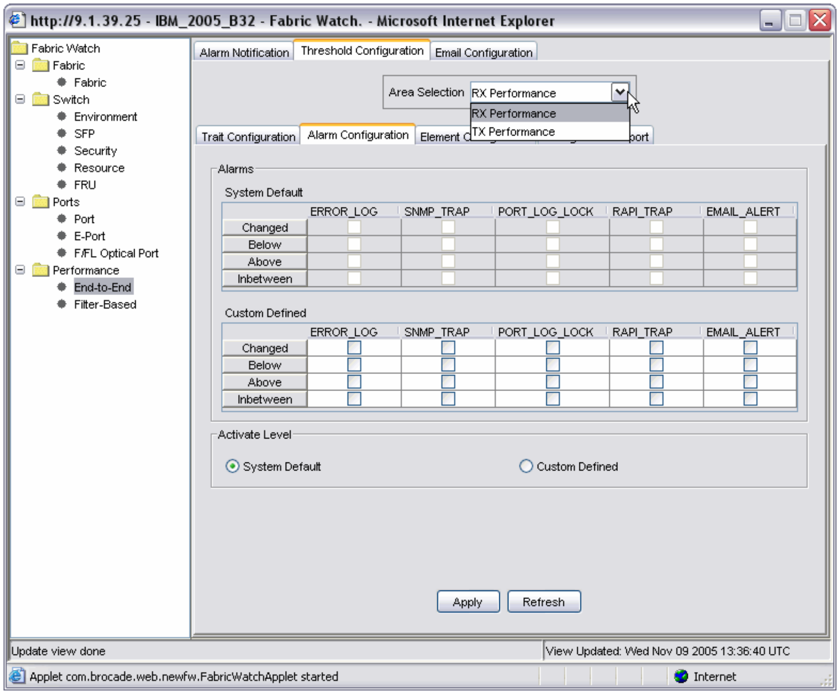
View Updated: Thu Aug 17 2006 00:15:13 UTC

Applet com.brocade.web.newfw.FabricWatchApplet started

Figure 1-129 Port Thresholds

Use the **Threshold Configuration** tab to view and configure End-to-End thresholds for the Performance class currently selected in the organizational tree on the left side of the window.

Be aware that you must define the SID/DID pair through the Performance Monitor before you can monitor the threshold in the End-to-End class. The **Threshold Configuration** tab for the End-to-End Thresholds is shown in Figure 1-130.


http://9.1.39.25 - IBM_2005_B32 - Fabric Watch. - Microsoft Internet Explorer
Fabric Watch
Fabric
Fabric
Switch
Environment
SFP
Security
Resource
FRU
Ports
Port
E-Port
F/FL Optical Port
Performance
End-to-End
Filter-Based
Alarm Notification
Threshold Configuration
Email Configuration
RX Performance
TX Performance
Trait Configuration
Alarm Configuration
Element C
ort
Apply
Refresh
Internet

Area Selection: RX Performance

Alarms

System Default

	ERROR_LOG	SNMP_TRAP	PORT_LOG_LOCK	RAPI_TRAP	EMAIL_ALERT
Changed	☐	☐	☐	☐	☐
Below	☐	☐	☐	☐	☐
Above	☐	☐	☐	☐	☐
Inbetween	☐	☐	☐	☐	☐

Custom Defined

	ERROR_LOG	SNMP_TRAP	PORT_LOG_LOCK	RAPI_TRAP	EMAIL_ALERT
Changed	☐	☐	☐	☐	☐
Below	☐	☐	☐	☐	☐
Above	☐	☐	☐	☐	☐
Inbetween	☐	☐	☐	☐	☐

Activate Level

● System Default ○ Custom Defined

Update view done

View Updated: Wed Nov 09 2005 13:36:40 UTC

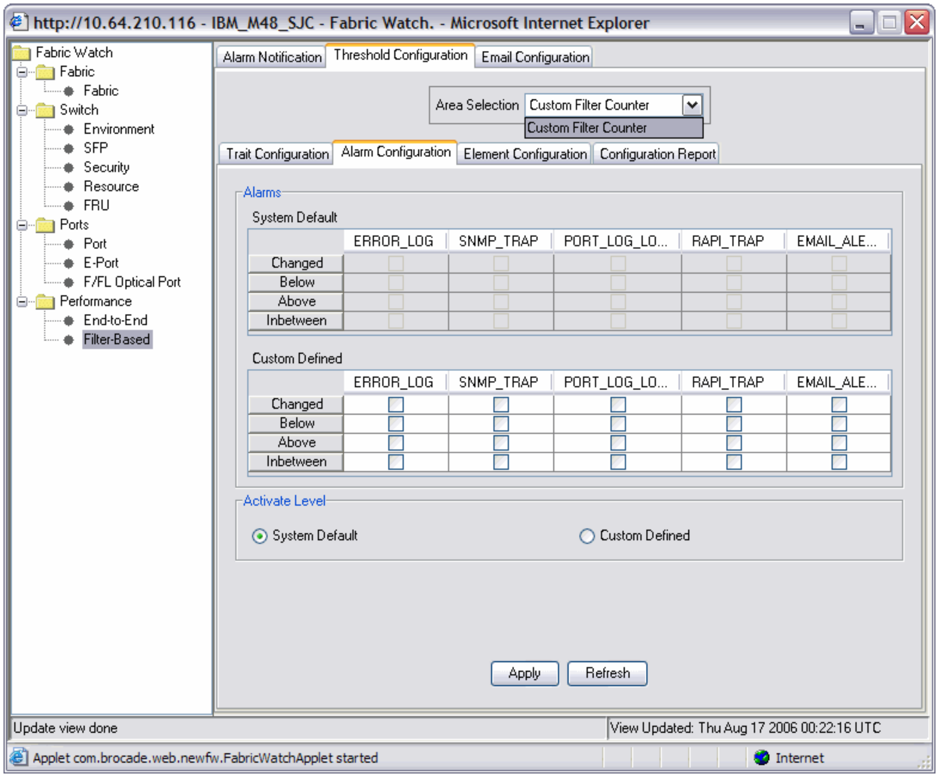
Applet com.brocade.web.newfw.FabricWatchApplet started

Figure 1-130 Thresholds tab for End-to-End

Use the **Threshold Configuration** tab to view and configure Filter-based thresholds for the Performance class currently selected in the organizational tree on the left side of the window as shown in Figure 1-131.

> **Note:** The filter type must be predefined in the Performance Monitor before you can use the Filter-Based thresholds.

The **Configure Thresholds** tab is shown in Figure 1-131.


http://10.64.210.116 - IBM_M48_SJC - Fabric Watch. - Microsoft Internet Explorer
Fabric Watch
Fabric
Fabric
Switch
Environment
SFP
Security
Resource
FRU
Ports
Port
E-Port
F/FL Optical Port
Performance
End-to-End
Filter-Based
Alarm Notification
Threshold Configuration
Email Configuration
Trait Configuration
Alarm Configuration
Element Configuration
Configuration Report
Apply
Refresh
Internet

Area Selection: Custom Filter Counter

Alarms

System Default

	ERROR_LOG	SNMP_TRAP	PORT_LOG_LO...	RAPI_TRAP	EMAIL_ALE...
Changed	☐	☐	☐	☐	☐
Below	☐	☐	☐	☐	☐
Above	☐	☐	☐	☐	☐
Inbetween	☐	☐	☐	☐	☐

Custom Defined

	ERROR_LOG	SNMP_TRAP	PORT_LOG_LO...	RAPI_TRAP	EMAIL_ALE...
Changed	☐	☐	☐	☐	☐
Below	☐	☐	☐	☐	☐
Above	☐	☐	☐	☐	☐
Inbetween	☐	☐	☐	☐	☐

Activate Level

● System Default ○ Custom Defined

Update view done

View Updated: Thu Aug 17 2006 00:22:16 UTC

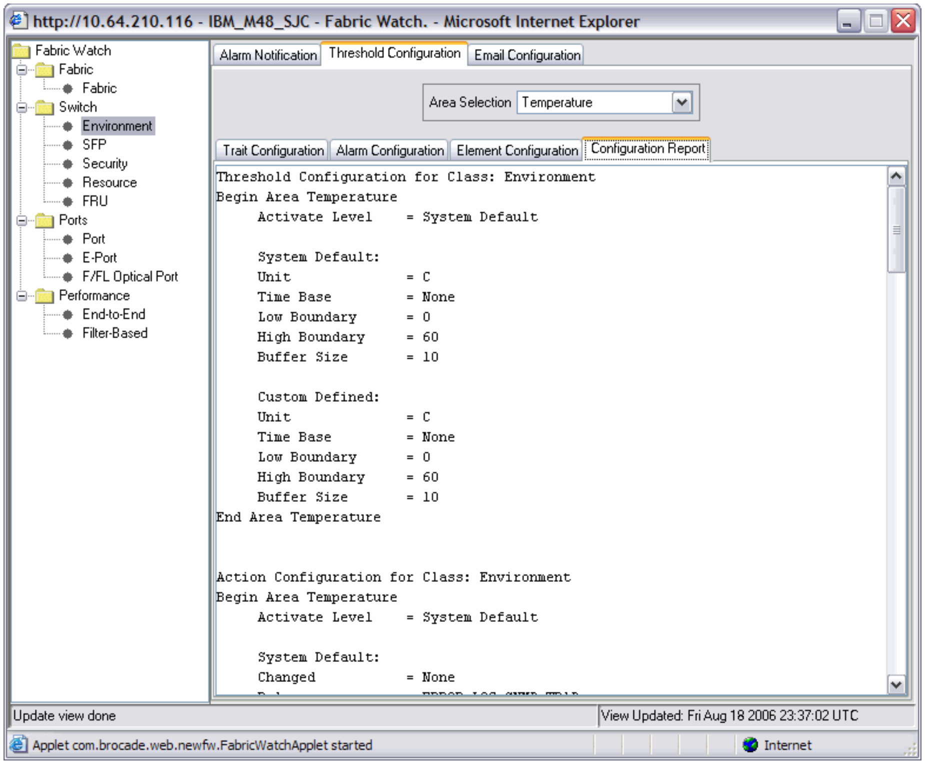
Applet com.brocade.web.newfw.FabricWatchApplet started

Figure 1-131 Thresholds tab with filter-based class

Configuration Report tab

Use the **Configuration Report** tab to view the current Fabric Watch threshold parameters for the area selected in the Fabric Watch tree.

The **Configuration Report** tab is shown in Figure 1-132.


http://10.64.210.116 - IBM_M48_SJC - Fabric Watch. - Microsoft Internet Explorer
Fabric Watch
Fabric
Fabric
Switch
Environment
SFP
Security
Resource
FRU
Ports
Port
E-Port
F/FL Optical Port
Performance
End-to-End
Filter-Based
Alarm Notification
Threshold Configuration
Email Configuration
Area Selection
Temperature
Trait Configuration
Alarm Configuration
Element Configuration
Configuration Report
Internet

```
Threshold Configuration for Class: Environment
Begin Area Temperature
     Activate Level     = System Default

     System Default:
     Unit               = C
     Time Base          = None
     Low Boundary       = 0
     High Boundary      = 60
     Buffer Size        = 10

     Custom Defined:
     Unit               = C
     Time Base          = None
     Low Boundary       = 0
     High Boundary      = 60
     Buffer Size        = 10
End Area Temperature


Action Configuration for Class: Environment
Begin Area Temperature
     Activate Level     = System Default

     System Default:
     Changed            = None
```

Update view done

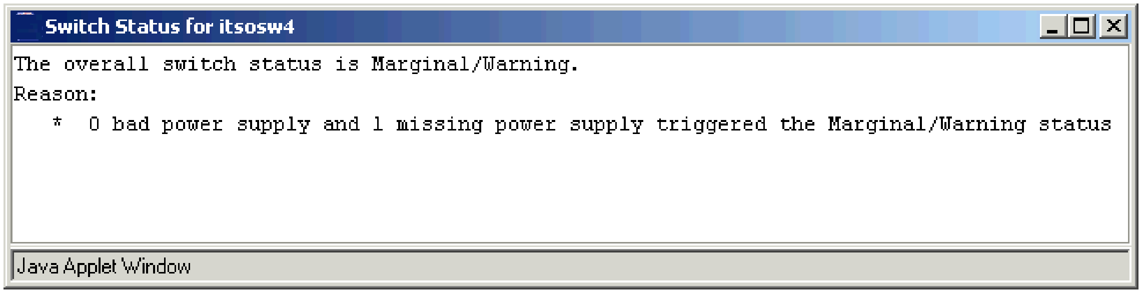
View Updated: Fri Aug 18 2006 23:37:02 UTC

Applet com.brocade.web.newfw.FabricWatchApplet started

Figure 1-132 Configuration report

Modifying settings for switches with one power supply

The IBM default settings for Fabric Watch cause a switch with a single power supply to appear yellow in the WebTools, indicating a *MARGINAL* status. The status can also be obtained by clicking the **Status button** in the switch view; this opens a window describing the cause of our marginal state, as shown in Figure 1-133.



```
The overall switch status is Marginal/Warning.
Reason:
   *  0 bad power supply and 1 missing power supply triggered the Marginal/Warning status
```

Figure 1-133 Checking the switch status

The switch status can be changed to *HEALTHY* using a Telnet connection. We use the **`switchstatusshow`** command to display the current health of the switch. After using **`switchstatuspolicyset`** to clear the current condition, we again use **`switchstatusshow`** to demonstrate that a switch with only one power supply is then shown with a *HEALTHY* status. See Example 1-21 for details.

Example 1-21 Using switchStatusPolicySet to clear unnecessary marginal status

```
IBM_2005_B32:admin> switchstatusshow
Switch Health Report                        Report time: 11/21/2006 10:27:20 AM
Switch Name: IBM_2005_B32
IP address:9.1.39.25
SwitchState:MARGINAL
Duration:00:01

Power supplies monitorMARGINAL
Temperatures monitor  HEALTHY
Fans monitor          HEALTHY
Flash monitor         HEALTHY
Marginal ports monitorHEALTHY
Faulty ports monitor  HEALTHY
Missing SFPs monitor  HEALTHY


All ports are healthy
IBM_2005_B32:admin> switchstatuspolicyset

To change the overall switch status policy parameters

The current overall switch status policy parameters:
                   Down    Marginal
 ----------------------------------
     PowerSupplies    2           1
      Temperatures    2           1
              Fans    2           1
             Flash    0           1
     MarginalPorts    2           1
       FaultyPorts    2           1
       MissingSFPs    0           0

Note that the value, 0, for a parameter, means that it is
NOT used in the calculation.
** In addition, if the range of settable values in the prompt is (0..0),
** the policy parameter is NOT applicable to the switch.
** Simply hit the Return key.


The minimum number of
  Bad PowerSupplies contributing to DOWN status: (0..2) [2] 0
  Bad PowerSupplies contributing to MARGINAL status: (0..2) [1] 0
  Bad Temperatures contributing to DOWN status: (0..5) [2]
  Bad Temperatures contributing to MARGINAL status: (0..5) [1]
  Bad Fans contributing to DOWN status: (0..3) [2]
  Bad Fans contributing to MARGINAL status: (0..3) [1]
  Out of range Flash contributing to DOWN status: (0..1) [0]
  Out of range Flash contributing to MARGINAL status: (0..1) [1]
  MarginalPorts contributing to DOWN status: (0..32) [2]
  MarginalPorts contributing to MARGINAL status: (0..32) [1]
  FaultyPorts contributing to DOWN status: (0..32) [2]
  FaultyPorts contributing to MARGINAL status: (0..32) [1]
  MissingSFPs contributing to DOWN status: (0..32) [0]
  MissingSFPs contributing to MARGINAL status: (0..32) [0]

Policy parameter set has been changed

IBM_2005_B32:admin> switchstatusshow
Switch Health Report                        Report time: 11/21/2006 10:28:24 AM
Switch Name: IBM_2005_B32
IP address:9.1.39.25
SwitchState:HEALTHY
Duration:00:00

Power supplies monitorHEALTHY
Temperatures monitor  HEALTHY
Fans monitor          HEALTHY
Flash monitor         HEALTHY
Marginal ports monitorHEALTHY
Faulty ports monitor  HEALTHY
Missing SFPs monitor  HEALTHY


All ports are healthy
IBM_2005_B32:admin>
```

To change the default settings, we issue the command: **`switchstatuspolicyset`**.

The first section of response to the command is the same as if we had issued the **`switchstatuspolicyshow`** command and displays a list of the current settings. Here we can see that the *PowerSupplies* line is defined to be Marginal if the switch is powered by one power supply. These default settings assume that the switch has two power supplies and that one has failed. Obviously, for a switch purchased with a single power supply, this is not valid.

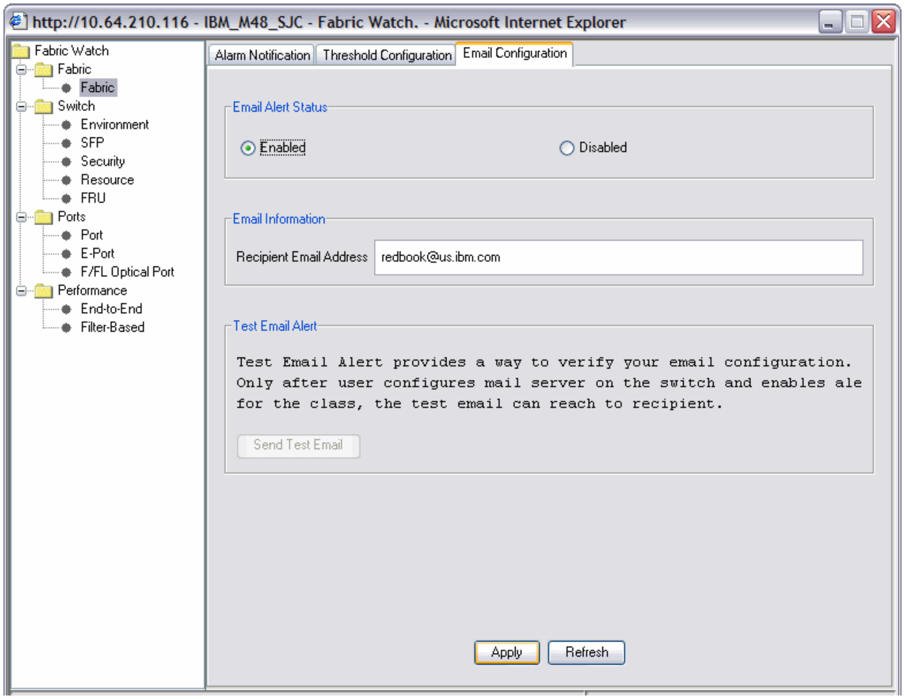
We are then prompted to enter the new values for each setting, starting with the *DOWN* value for the Faulty Ports, then the *MARGINAL* value for Faulty Ports. We press Enter to use default values; we are prompted for the next setting, and eventually, for the Power supply *DOWN* and *MARGINAL* values.

We enter zero for the number of *bad power supplies contributing to the DOWN status* and zero for the number of *bad power supplies contributing to the MARGINAL status*. Indeed, because we are working with only one power supply, if it goes down, then the whole switch goes down. There is no marginal status.

At the bottom of the Telnet display, after running the **`switchstatusshow`** command, we can see that the chassis status has changed from *MARGINAL* to *HEALTHY*.

Email Configuration

Use the **Email Configuration** tab to configure the destination e-mail ID to receive any alerts selected in the threshold configuration to deliver to e-mail as shown in Figure 1-134. Also on this tab, we are able to generally enable or disable the e-mail function for fabric Watch alerts, and send a test e-mail to ensure that the function is working.


http://10.64.210.116 - IBM_M48_SJC - Fabric Watch. - Microsoft Internet Explorer
Fabric Watch
Fabric
Fabric
Switch
Environment
SFP
Security
Resource
FRU
Ports
Port
E-Port
F/FL Optical Port
Performance
End-to-End
Filter-Based
Alarm Notification
Threshold Configuration
Email Configuration
Send Test Email
Apply
Refresh

Email Alert Status

● Enabled ○ Disabled

Email Information

Recipient Email Address: redbook@us.ibm.com

Test Email Alert

```
Test Email Alert provides a way to verify your email configuration.
Only after user configures mail server on the switch and enables ale
for the class, the test email can reach to recipient.
```

Figure 1-134 Email configuration

1.9 Fabric Manager

In the topics that follow we discuss Fabric Manager.

1.9.1 Fabric Manager requirements

Next we describe some of the requirements for Fabric Manager.

Switch requirements

Fabric Manager can be used to manage IBM TotalStorage SAN Switches that meet the following requirements:

- WebTools license is installed.
- Fabric OS v2.2 or greater is required. Fabric Manager can be used to manage switches with earlier versions of Fabric OS, but status and event information are not available.

System requirements for client and server machines

The system requirements for installing Fabric Manager client and server machines are listed in Table 1-25. These services can also be installed on a Solaris machine; for details on this, refer to the *Brocade Fabric Manager Administrator’s Guide,* 53-1000042-01.

Table 1-25 System requirements for Fabric Manager client and server machines

Operating system	**Machine type**	**Requirements**		
		1-512 Ports (1-20 Switches)	**513-1280 Ports (12-50 Switches)**	**1281-2560 Ports (51-80 Switches)**
Windows and Linux	Client	800Mhz CPU 256 MB RAM 512MB virtual memory	1.5Ghz CPU 512MB RAM 512MB virtual memory	1.5Ghz CPU 512MB RAM 512MB virtual memory
	Server	1.8Ghz P4 1 GB RAM 512MB virtual memory	2.0 GHz P4 1.5GB RAM 512MB virtual memory	2x3 GHz P4 CPU 2.5GB RAM 1GB virtual memory
	Combined	2Ghz P4 1.5 GB RAM 1 GB virtual memory	2x3GHz P4 CPU 2GB RAM 1GB virtual memory	Not recommended

Along with the general system requirements, the following items are necessary for the correct installation and operation of Fabric Manager:

- One of the following operating systems:
  - Fabric Manager Server: Windows 2000 Server SP4, Windows 2003 Server SP1, or Windows XP SP2
  - Fabric Manager Client: Windows NT® 4.0, Windows 2000, Solaris 2.7, or Solaris 2.8
  - Red Hat Linux AS 3.0 (x86 only)
  - Solaris 8/9/10 (Sparc only)
- 400 MB of free disk space (Windows) and 500 MB Linux for the installation
- 2 GB of free disk space for small and medium sized SANs or 10GB for large SANs

- One of the following Web browsers with Java plug in 1.4.2_08 or higher:
  - Mozilla 1.7.8
  - Internet Explorer 6.0

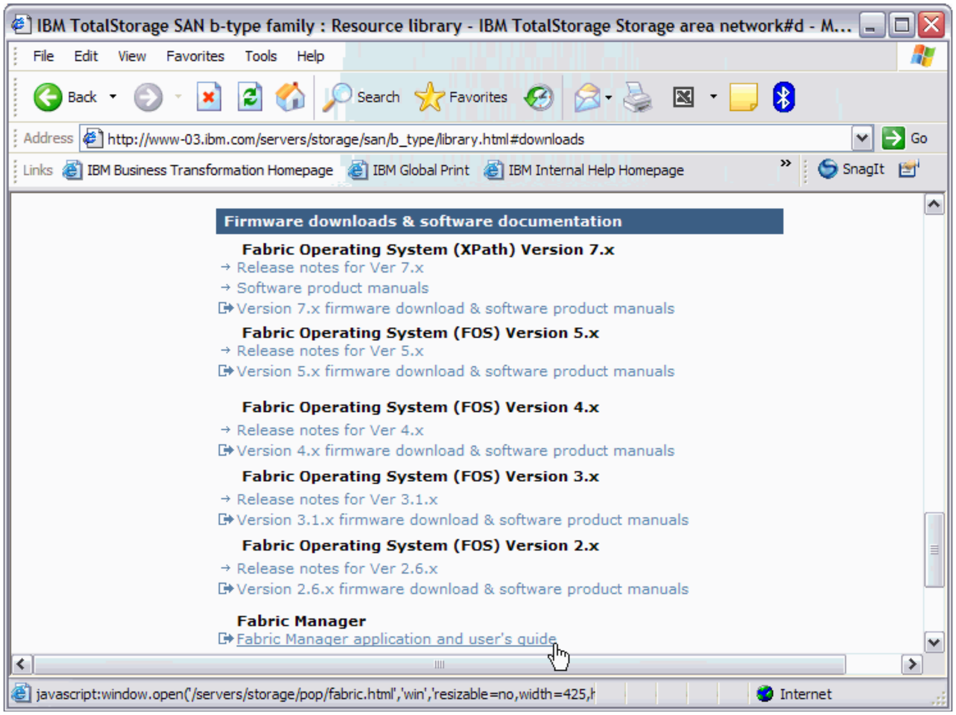
> **Important:** In order to run the Fabric Manager client, it must be running the same version of Fabric Manager as the server.

1.9.2 Installing Fabric Manager

You can download the latest level of Fabric Manager from the following link:

`http://www-1.ibm.com/servers/storage/san/b_type/library.html#downloads`

We show this in Figure 1-135.


IBM TotalStorage SAN b-type family : Resource library - IBM TotalStorage Storage area network#d - M...
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://www-03.ibm.com/servers/storage/san/b_type/library.html#downloads
Go
Links
IBM Business Transformation Homepage
IBM Global Print
IBM Internal Help Homepage
SnagIt
Internet

Firmware downloads & software documentation

Fabric Operating System (XPath) Version 7.x

→ Release notes for Ver 7.x
→ Software product manuals
Version 7.x firmware download & software product manuals

Fabric Operating System (FOS) Version 5.x

→ Release notes for Ver 5.x
Version 5.x firmware download & software product manuals

Fabric Operating System (FOS) Version 4.x

→ Release notes for Ver 4.x
Version 4.x firmware download & software product manuals

Fabric Operating System (FOS) Version 3.x

→ Release notes for Ver 3.1.x
Version 3.1.x firmware download & software product manuals

Fabric Operating System (FOS) Version 2.x

→ Release notes for Ver 2.6.x
Version 2.6.x firmware download & software product manuals

Fabric Manager

Fabric Manager application and user's guide

javascript:window.open('/servers/storage/pop/fabric.html','win','resizable=no,width=425,h

Figure 1-135 Pointer to Fabric Manager download

On selecting the Fabric Manager link, you are advised that you are leaving the IBM Web site.

From here we are redirected to the Brocade Web site. We can download whichever Fabric Manager version matches the FOS that we are running, as shown in Figure 1-136.

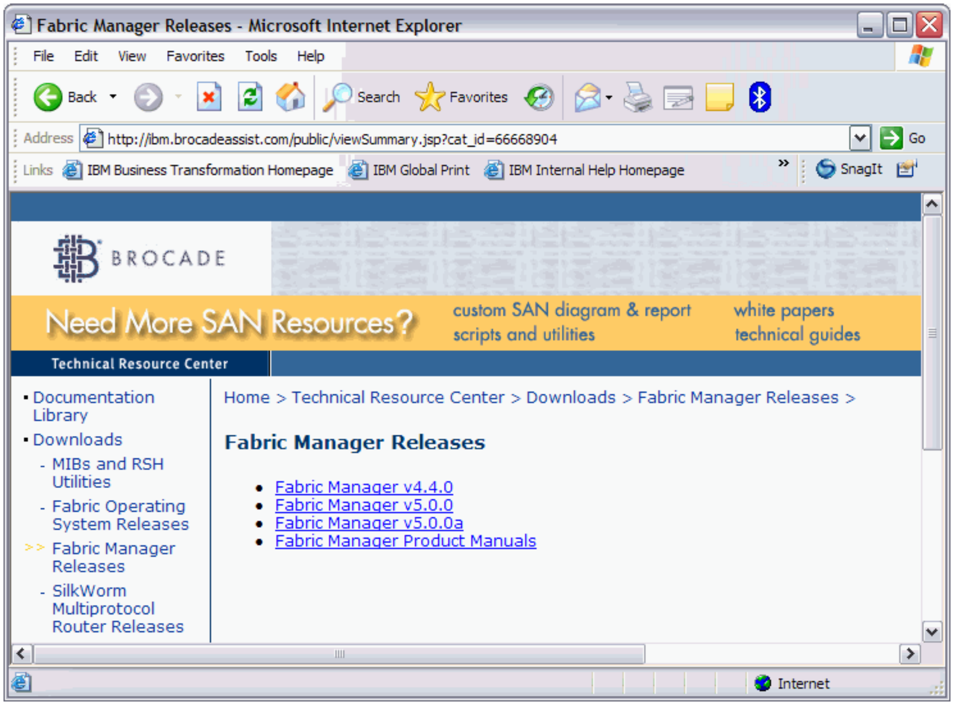

Fabric Manager Releases - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://ibm.brocadeassist.com/public/viewSummary.jsp?cat_id=66668904
Go
Links IBM Business Transformation Homepage IBM Global Print IBM Internal Help Homepage
SnagIt
BROCADE
Need More SAN Resources?
custom SAN diagram & report
scripts and utilities
white papers
technical guides
Technical Resource Center
Documentation Library
Downloads
MIBs and RSH Utilities
Fabric Operating System Releases
Fabric Manager Releases
SilkWorm Multiprotocol Router Releases
Home > Technical Resource Center > Downloads > Fabric Manager Releases >
Fabric Manager Releases
Fabric Manager v4.4.0
Fabric Manager v5.0.0
Fabric Manager v5.0.0a
Fabric Manager Product Manuals
Internet

Figure 1-136 Brocade download Fabric manager

For our purposes, we downloaded the Fabric Manager 5.1.0 for Windows. The installation instructions are easy to follow, with only a small number of decisions required, which we detail here:

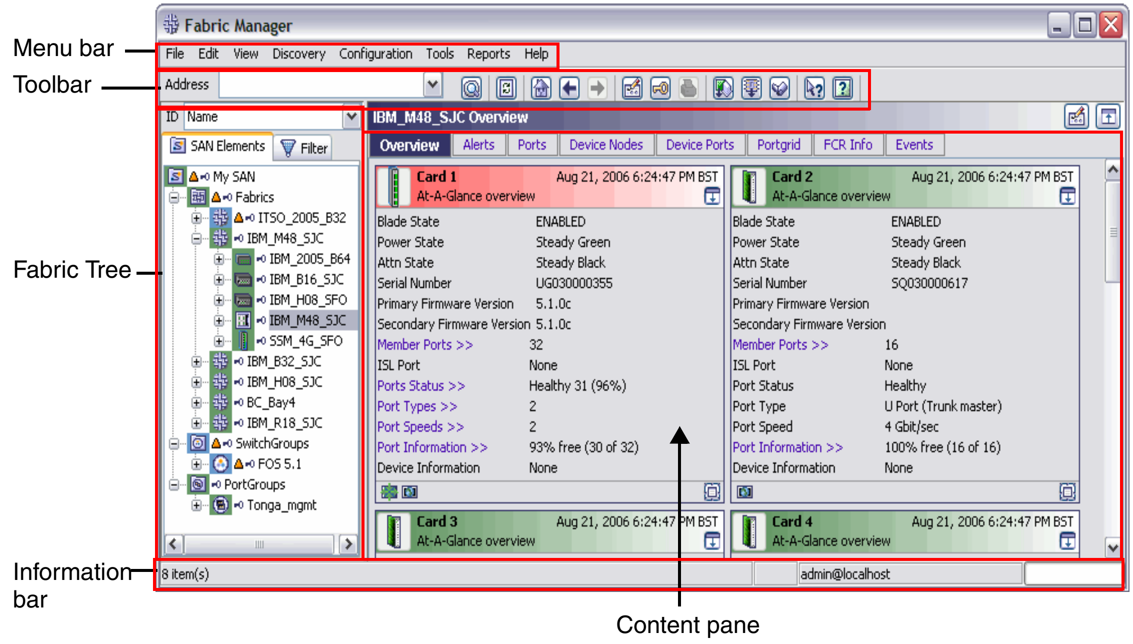
- Type of installation required:
  - Server and client
  - Client
  - Server
- Destination folder
- FTP server:
  - Built in
  - External
- Starting port number (default 24600 - 8 ports required)
- Server authentication method:
  - Windows domain or work group
  - Radius authentication
  - Switch based authentication
- Select the size of SAN to be managed:
  - Small (for managing up to 512 ports, 1-20 domains)
  - Medium (for managing 513 to 1280 ports, 21-50 domains)
  - Large (for managing 1281 to 2560 ports, 51-80 domains)

Important: The FTP server used by Fabric manager must be local to the Fabric Manager server. That is, if you use an external FTP server, it must run from the Fabric Manager server.

1.9.3 Fabric Manager Interface overview

Here we provide a high level guide to using the Fabric Manager interface. Figure 1-137 shows the general Fabric Manager window layout.

The menu bar contains a selection of drop down menus from which specific Fabric Manager tasks can be run. The Toolbar provides a short cut to several of the most commonly used features, hovering the mouse pointer over the buttons generates a brief pop-up description of what they do. The Fabric Tree displays the discovered switches, fabrics and ports as well as any switch or port groups you have created. The Contents Pane changes according to the selected Fabric manager option.


Menu bar
Toolbar
Fabric Tree
Information bar
Content pane
Fabric Manager
File Edit View Discovery Configuration Tools Reports Help
Address
ID Name
SAN Elements
Filter
My SAN
Fabrics
ITSO_2005_B32
IBM_M48_SJC
IBM_2005_B64
IBM_B16_SJC
IBM_H08_SFO
IBM_M48_SJC
SSM_4G_SFO
IBM_B32_SJC
IBM_H08_SJC
BC_Bay4
IBM_R18_SJC
SwitchGroups
FOS 5.1
PortGroups
Tonga_mgmt
IBM_M48_SJC Overview
Overview Alerts Ports Device Nodes Device Ports Portgrid FCR Info Events
8 item(s)
admin@localhost

Card 1 At-A-Glance overview — Aug 21, 2006 6:24:47 PM BST

Blade State	ENABLED
Power State	Steady Green
Attn State	Steady Black
Serial Number	UG030000355
Primary Firmware Version	5.1.0c
Secondary Firmware Version	5.1.0c
Member Ports >>	32
ISL Port	None
Ports Status >>	Healthy 31 (96%)
Port Types >>	2
Port Speeds >>	2
Port Information >>	93% free (30 of 32)
Device Information	None

Card 2 At-A-Glance overview — Aug 21, 2006 6:24:47 PM BST

Blade State	ENABLED
Power State	Steady Green
Attn State	Steady Black
Serial Number	SQ030000617
Primary Firmware Version	
Secondary Firmware Version	
Member Ports >>	16
ISL Port	None
Port Status	Healthy
Port Type	U Port (Trunk master)
Port Speed	4 Gbit/sec
Port Information >>	100% free (16 of 16)
Device Information	None

Card 3 At-A-Glance overview — Aug 21, 2006 6:24:47 PM BST

Card 4 At-A-Glance overview — Aug 21, 2006 6:24:47 PM BST

Figure 1-137 Fabric Manager window overview

The Toolbar icons are detailed in Figure 1-138. From left to right, these are:

- Subnet Scan
- Refresh
- Home
- Previous
- Next
- Configure Fabric Manager options
- Fabric Login
- Print
- Firmware Download to HBAs
- Firmware Download to switches
- Sequenced reboot
- Context sensitive help
- Help

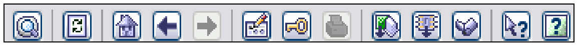


Figure 1-138 Fabric manager Toolbar

1.9.4 Launching Fabric Manager

Here we demonstrate how to use the Fabric Manager in a Windows environment.

Launching in Windows

We can launch Fabric Manager when Fabric Manager and the Java plug-in are both installed on the workstation.

To launch Fabric Manager:

Select **Start** → **Programs** → **FabricManager** → **FabricManager**

We first get a logon window where we use our Windows domain userid and password.

1.9.5 Implementing Fabric Manager

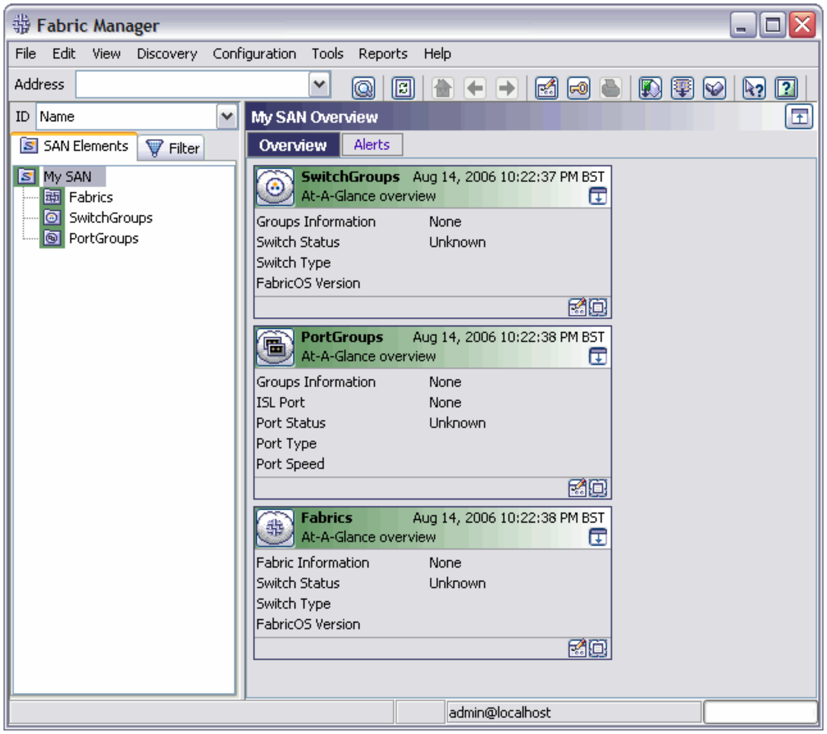
In the following paragraphs, we go through some of the more useful functions. For more options and a detailed description of Fabric Manager, refer to the *Brocade Fabric Manager Administrator's Guide*, 53-1000042-01.

Fabric Manager view

The Fabric Manager detail view is the first view that displays when we launch Fabric Manager. It provides access to specific information about the fabric and switches through a panel that represents each switch. Every switch in the fabric, including any unlicensed switches, is represented by a switch panel in Fabric Manager view.

However, only switches with a WebTools license can be managed from Fabric Manager. To add a license for an unlicensed switch, click the corresponding switch icon in Fabric Manager view, and a license window automatically displays.

The initial Fabric Manager view opens as shown in Figure 1-139.


Fabric Manager
File
Edit
View
Discovery
Configuration
Tools
Reports
Help
Address
ID
Name
SAN Elements
Filter
My SAN
Fabrics
SwitchGroups
PortGroups
My SAN Overview
Overview
Alerts
admin@localhost

SwitchGroups Aug 14, 2006 10:22:37 PM BST
At-A-Glance overview

Groups Information None
Switch Status Unknown
Switch Type
FabricOS Version

PortGroups Aug 14, 2006 10:22:38 PM BST
At-A-Glance overview

Groups Information None
ISL Port None
Port Status Unknown
Port Type
Port Speed

Fabrics Aug 14, 2006 10:22:38 PM BST
At-A-Glance overview

Fabric Information None
Switch Status Unknown
Switch Type
FabricOS Version

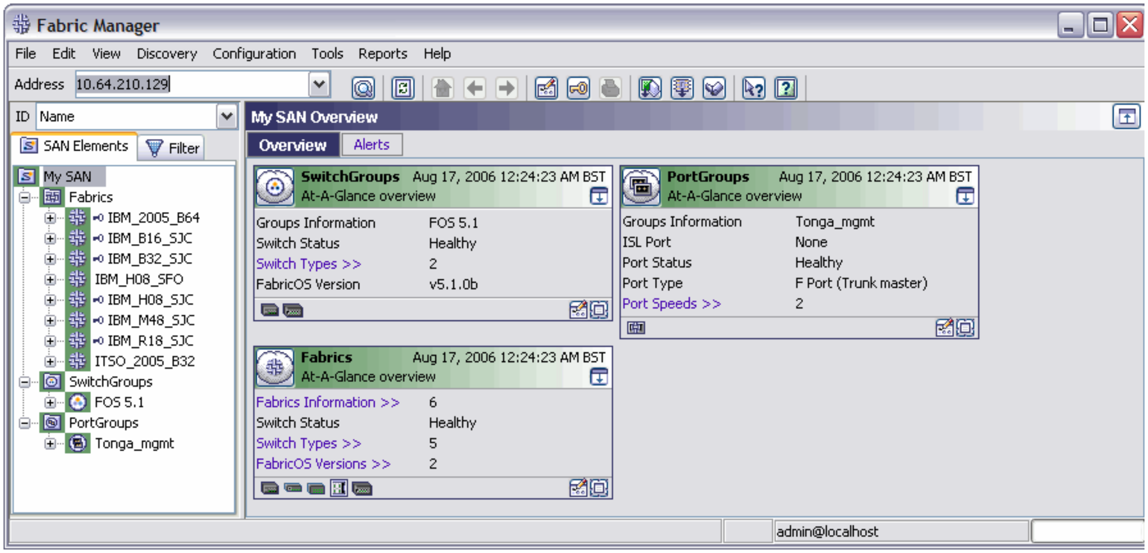
Figure 1-139 Fabric Manager address window

1. Type the switch name or IP address in the Address field.

Note: When working in a multiswitch environment, we recommend that you enter the IP address of the switch with the highest port count and highest level of firmware. If an M48 is installed, then use that IP address.

2. Press Enter to submit the address.

After we add the IP addresses of the switches we want to manage with Fabric Manager, we can now see details as shown in Figure 1-140.


Fabric Manager
File Edit View Discovery Configuration Tools Reports Help
Address 10.64.210.129
ID Name
SAN Elements
Filter
My SAN
Fabrics
IBM_2005_B64
IBM_B16_SJC
IBM_B32_SJC
IBM_H08_SFO
IBM_H08_SJC
IBM_M48_SJC
IBM_R18_SJC
ITSO_2005_B32
SwitchGroups
FOS 5.1
PortGroups
Tonga_mgmt
My SAN Overview
Overview
Alerts
admin@localhost

SwitchGroups Aug 17, 2006 12:24:23 AM BST
At-A-Glance overview

Groups Information	FOS 5.1
Switch Status	Healthy
Switch Types >>	2
FabricOS Version	v5.1.0b

PortGroups Aug 17, 2006 12:24:23 AM BST
At-A-Glance overview

Groups Information	Tonga_mgmt
ISL Port	None
Port Status	Healthy
Port Type	F Port (Trunk master)
Port Speeds >>	2

Fabrics Aug 17, 2006 12:24:23 AM BST
At-A-Glance overview

Fabrics Information >>	6
Switch Status	Healthy
Switch Types >>	5
FabricOS Versions >>	2

Figure 1-140 Fabric manager view of multiple switches

The left-hand side is the SAN Elements Fabric tree panel. It is composed of a pull-down menu where we can select to display by *Name*, *IP*, *Domain ID*, *WWN*, the *Navigation Tree control*, and two tabs (*SAN elements* and *Filter*).

The Navigation Tree control of the SAN Elements panel displays various nodes, such as Fabrics, Groups, Reboot Groups, Devices, Switches, Ports, and so on.

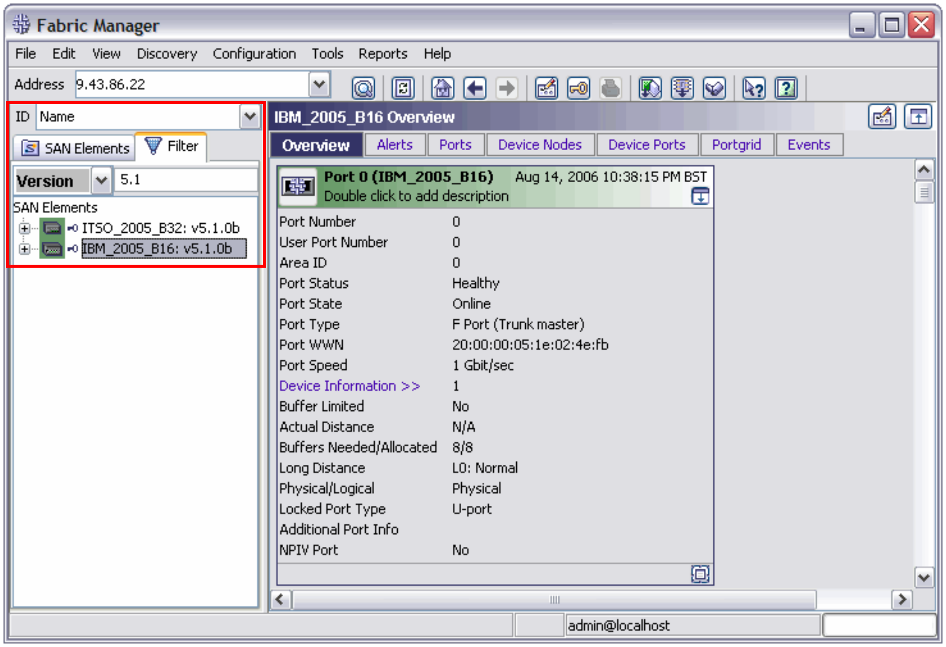
By selecting one of the options from the pulldown menu, we can modify the display of the SAN elements on the SAN Elements panel:

- **Name:** Displays the defined switch name.
- **IP:** Displays the switch IP address.
- **WWN:** Displays the switch WWN.
- **Domain ID:** Displays each switch’s domain ID.

The Filter panel allows us to filter the browser display and show only switches matching one of the following criteria:

- IP
- Name
- Type
- Version
- WWN
- Domain ID

To filter the display, choose one of the criteria in the list box, type the desired value in the edit box, and press Enter. This displays a window similar to Figure 1-141.


Fabric Manager
File Edit View Discovery Configuration Tools Reports Help
Address
ID Name
SAN Elements
Filter
IBM_2005_B16 Overview
Overview Alerts Ports Device Nodes Device Ports Portgrid Events
admin@localhost

Address 9.43.86.22

Version 5.1

SAN Elements
- ITSO_2005_B32: v5.1.0b
- IBM_2005_B16: v5.1.0b

Port 0 (IBM_2005_B16) Aug 14, 2006 10:38:15 PM BST
Double click to add description

Port Number	0
User Port Number	0
Area ID	0
Port Status	Healthy
Port State	Online
Port Type	F Port (Trunk master)
Port WWN	20:00:00:05:1e:02:4e:fb
Port Speed	1 Gbit/sec
Device Information >>	1
Buffer Limited	No
Actual Distance	N/A
Buffers Needed/Allocated	8/8
Long Distance	L0: Normal
Physical/Logical	Physical
Locked Port Type	U-port
Additional Port Info	
NPIV Port	No

Figure 1-141 Applying filter to SAN elements display

In Figure 1-141, we want to restrict the display to devices running firmware version v5.1.

The right-hand side of the Fabric View window is the Switch View portion of the Fabric View. We can use it to manage individual switches.

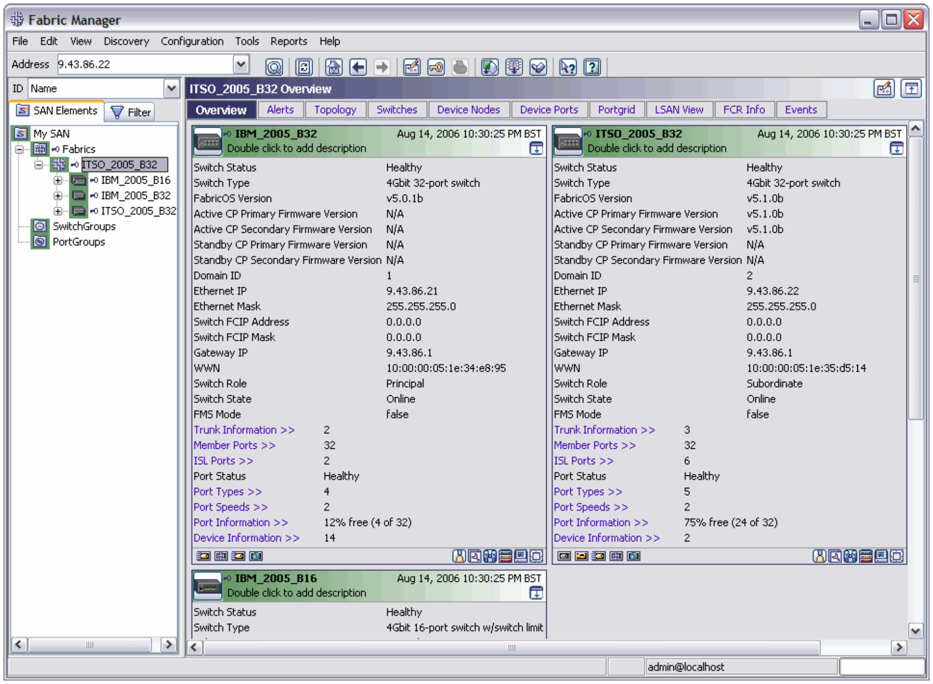
From this view, we can access switch specific operations such as:

- Switch events
- Switch settings
- Telnet window
- Switch front panel view

Launching the Switch View in Fabric Manager actually launches the WebTools interface for that switch.

Depending on our selection in the navigation tree, the Switch View displays either a fabric icon or individual switch icons.

Figure 1-142 shows the window display at a fabric level.


Fabric Manager
File Edit View Discovery Configuration Tools Reports Help
Address 9.43.86.22
ID Name
SAN Elements
Filter
My SAN
Fabrics
ITSO_2005_B32
IBM_2005_B16
IBM_2005_B32
ITSO_2005_B32
SwitchGroups
PortGroups
ITSO_2005_B32 Overview
Overview Alerts Topology Switches Device Nodes Device Ports Portgrid LSAN View FCR Info Events
admin@localhost

IBM_2005_B32 Aug 14, 2006 10:30:25 PM BST
Double click to add description

Switch Status	Healthy
Switch Type	4Gbit 32-port switch
FabricOS Version	v5.0.1b
Active CP Primary Firmware Version	N/A
Active CP Secondary Firmware Version	N/A
Standby CP Primary Firmware Version	N/A
Standby CP Secondary Firmware Version	N/A
Domain ID	1
Ethernet IP	9.43.86.21
Ethernet Mask	255.255.255.0
Switch FCIP Address	0.0.0.0
Switch FCIP Mask	0.0.0.0
Gateway IP	9.43.86.1
WWN	10:00:00:05:1e:34:e8:95
Switch Role	Principal
Switch State	Online
FMS Mode	false
Trunk Information >>	2
Member Ports >>	32
ISL Ports >>	2
Port Status	Healthy
Port Types >>	4
Port Speeds >>	2
Port Information >>	12% free (4 of 32)
Device Information >>	14

ITSO_2005_B32 Aug 14, 2006 10:30:25 PM BST
Double click to add description

Switch Status	Healthy
Switch Type	4Gbit 32-port switch
FabricOS Version	v5.1.0b
Active CP Primary Firmware Version	v5.1.0b
Active CP Secondary Firmware Version	v5.1.0b
Standby CP Primary Firmware Version	N/A
Standby CP Secondary Firmware Version	N/A
Domain ID	2
Ethernet IP	9.43.86.22
Ethernet Mask	255.255.255.0
Switch FCIP Address	0.0.0.0
Switch FCIP Mask	0.0.0.0
Gateway IP	9.43.86.1
WWN	10:00:00:05:1e:35:d5:14
Switch Role	Subordinate
Switch State	Online
FMS Mode	false
Trunk Information >>	3
Member Ports >>	32
ISL Ports >>	6
Port Status	Healthy
Port Types >>	5
Port Speeds >>	2
Port Information >>	75% free (24 of 32)
Device Information >>	2

IBM_2005_B16 Aug 14, 2006 10:30:25 PM BST
Double click to add description

Switch Status	Healthy
Switch Type	4Gbit 16-port switch w/switch limit

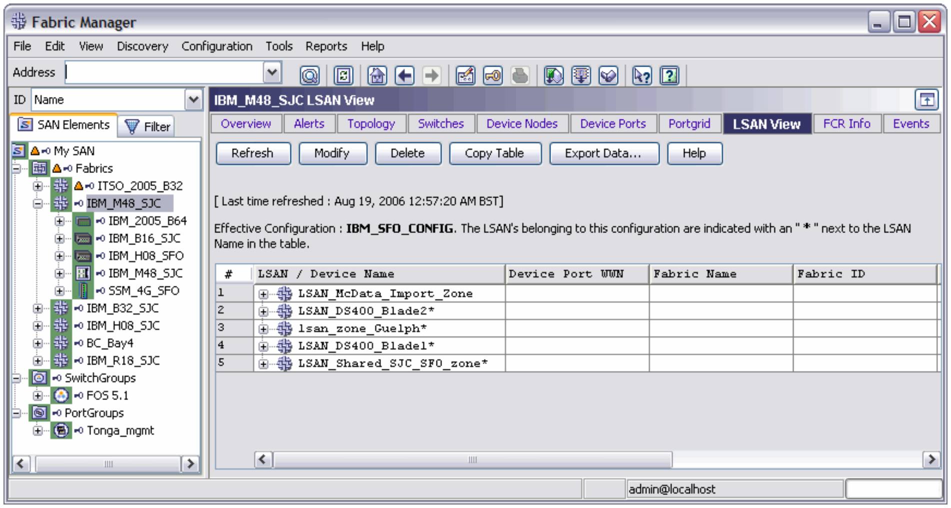
Figure 1-142 Fabric Detail

From the icons on the right hand side of this window, we can access fabric-wide operations such as:

- Fabric events
- Zone administration
- Name server
- Fabric topology
- LSAN details
- FCR details

> **Note:** The LSAN tab is only displayed when the fabric being monitored by Fabric Manager has a Fibre Channel router present.

Both LSANs - Logical Storage Area Networks and FCR - Fibre Channel Routing are covered in detail within the Redbooks publication, *SAN Multiprotocol Routing: An Introduction and Implementation*, SG24-7321. Figure 1-143 shows the high level Fabric Manager view of the LSANs within our fabric.


Fabric Manager
File Edit View Discovery Configuration Tools Reports Help
Address
ID Name
SAN Elements
Filter
My SAN
Fabrics
ITSO_2005_B32
IBM_M48_SJC
IBM_2005_B64
IBM_B16_SJC
IBM_H08_SFO
IBM_M48_SJC
SSM_4G_SFO
IBM_B32_SJC
IBM_H08_SJC
BC_Bay4
IBM_R18_SJC
SwitchGroups
FOS 5.1
PortGroups
Tonga_mgmt
IBM_M48_SJC LSAN View
Overview
Alerts
Topology
Switches
Device Nodes
Device Ports
Portgrid
LSAN View
FCR Info
Events
Refresh
Modify
Delete
Copy Table
Export Data...
Help
admin@localhost

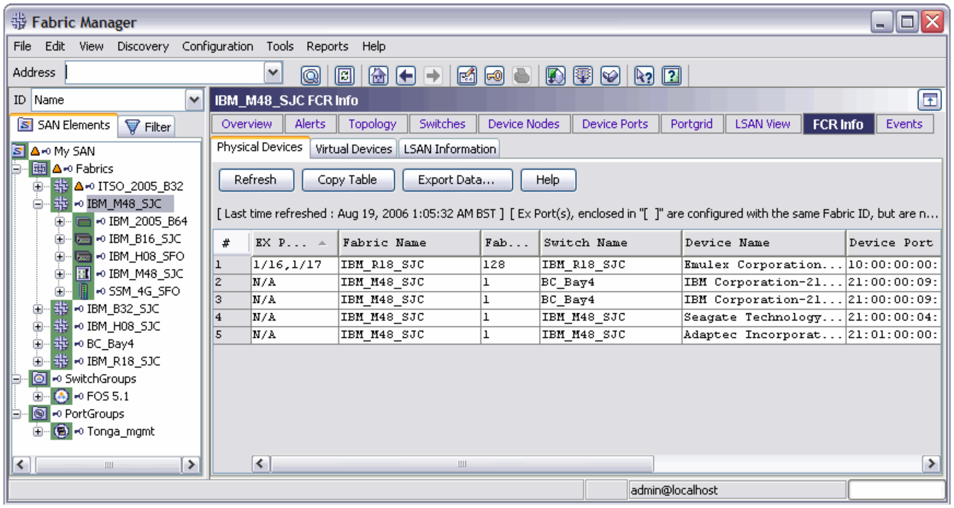
[Last time refreshed : Aug 19, 2006 12:57:20 AM BST]

Effective Configuration : **IBM_SFO_CONFIG**. The LSAN's belonging to this configuration are indicated with an " * " next to the LSAN Name in the table.

#	LSAN / Device Name	Device Port WWN	Fabric Name	Fabric ID
1	LSAN_McData_Import_Zone			
2	LSAN_DS400_Blade2*			
3	lsan_zone_Guelph*			
4	LSAN_DS400_Blade1*			
5	LSAN_Shared_SJC_SFO_zone*			

Figure 1-143 Viewing an LSAN within Fabric Manager

We can also view the FCR information as detailed in Figure 1-144.


Fabric Manager
File Edit View Discovery Configuration Tools Reports Help
Address
ID Name
SAN Elements
Filter
My SAN
Fabrics
ITSO_2005_B32
IBM_M48_SJC
IBM_2005_B64
IBM_B16_SJC
IBM_H08_SFO
IBM_M48_SJC
SSM_4G_SFO
IBM_B32_SJC
IBM_H08_SJC
BC_Bay4
IBM_R18_SJC
SwitchGroups
FOS 5.1
PortGroups
Tonga_mgmt
IBM_M48_SJC FCR Info
Overview
Alerts
Topology
Switches
Device Nodes
Device Ports
Portgrid
LSAN View
FCR Info
Events
Physical Devices
Virtual Devices
LSAN Information
Refresh
Copy Table
Export Data...
Help
admin@localhost

[Last time refreshed : Aug 19, 2006 1:05:32 AM BST] [Ex Port(s), enclosed in "[ ]" are configured with the same Fabric ID, but are n...

#	EX P...	Fabric Name	Fab...	Switch Name	Device Name	Device Port
1	1/16,1/17	IBM_R18_SJC	128	IBM_R18_SJC	Emulex Corporation...	10:00:00:00:
2	N/A	IBM_M48_SJC	1	BC_Bay4	IBM Corporation-21...	21:00:00:09:
3	N/A	IBM_M48_SJC	1	BC_Bay4	IBM Corporation-21...	21:00:00:09:
4	N/A	IBM_M48_SJC	1	IBM_M48_SJC	Seagate Technology...	21:00:00:04:
5	N/A	IBM_M48_SJC	1	IBM_M48_SJC	Adaptec Incorporat...	21:01:00:00:

Figure 1-144 Viewing FCR information within Fabric Manager

Creating logical groups

Logical groups allow us to operate on a set of switches that are not necessarily physically connected or part of the same fabric. For example, we could create logical groups according to the switch model.

Creating logical groups allows a greater degree of control by allowing switches to be grouped according to your requirements, including physical location, department, and function. It also simplifies the management of your fabrics, allowing you to group by switch model or firmware level, thus enabling firmware upgrades to multiple switches at the same time. Logical groups facilitate the activation of licenses across group members simultaneously, as well as simplifying the monitoring of your environment.

> **Tip:** Grouping switches by redundancy enables you to maintain fabric availability while carrying out changes to the other half.

We can create Port Groups, Switch Groups and Reboot groups. To create a Switch Group, we to go to File pull-down menu and select **Groups** and then **Edit Switch Groups**, or alternatively right-click the SwitchGroups item in the SAN Elements panel as shown in Figure 1-145.

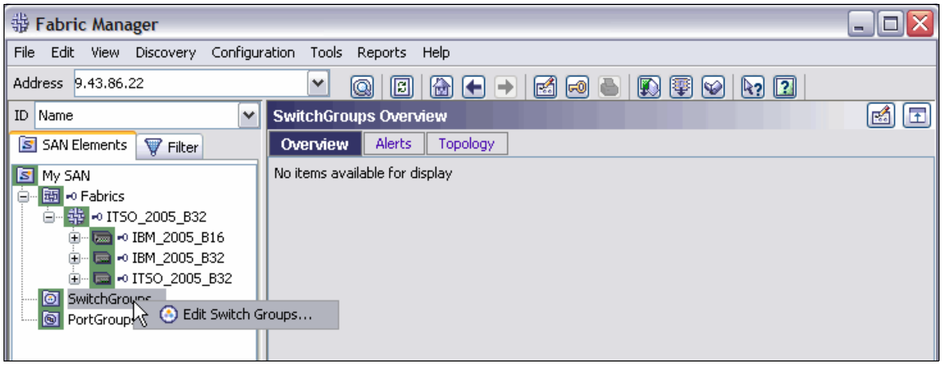
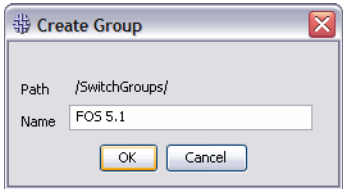

Fabric Manager
File
Edit
View
Discovery
Configuration
Tools
Reports
Help
Address
9.43.86.22
ID
Name
SwitchGroups Overview
SAN Elements
Filter
Overview
Alerts
Topology
No items available for display
My SAN
Fabrics
ITSO_2005_B32
IBM_2005_B16
IBM_2005_B32
ITSO_2005_B32
SwitchGroups
PortGroups
Edit Switch Groups...

Figure 1-145 Edit switch groups

This brings us to the **Edit Switch Group** panel, where we are able to perform various functions on the Switch groups as shown in Figure 1-146.


Create Group
OK
Cancel

Path /SwitchGroups/

Name FOS 5.1

Figure 1-146 Creating a new switch group

We are creating a new switch group, so we click the **Create** button and enter the name in the Create Group window shown in Figure 1-147.

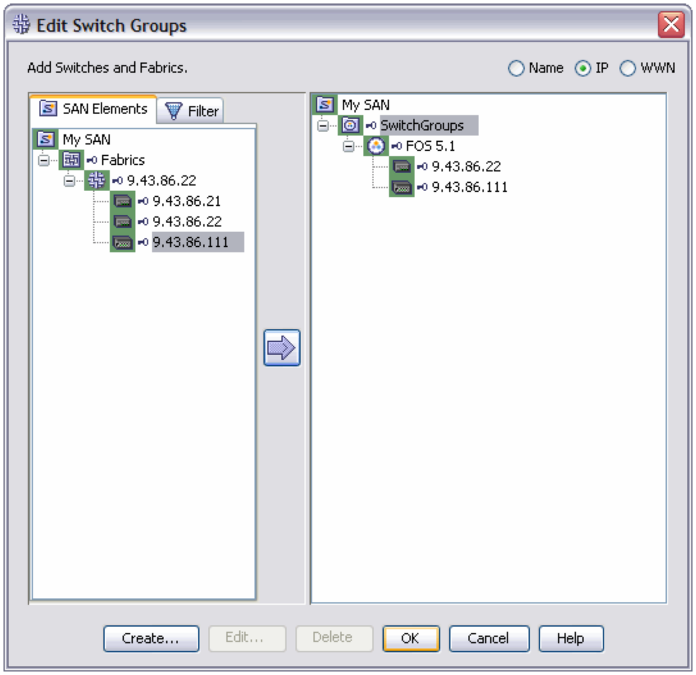

Edit Switch Groups
Add Switches and Fabrics.
○ Name ● IP ○ WWN
SAN Elements
Filter
My SAN
Fabrics
9.43.86.22
9.43.86.21
9.43.86.22
9.43.86.111
My SAN
SwitchGroups
FOS 5.1
9.43.86.22
9.43.86.111
Create...
Edit...
Delete
OK
Cancel
Help

Figure 1-147 Moving objects into the newly created group

When the group is created, we highlight it so that we can add members from the left hand side panel. To add members, we simply select them from the left hand side panel and then click the right arrow in the middle to add it to the group on the right hand side panel. This is shown in Figure 1-147.

Click **OK** to close this window. The group is now visible in the SwitchGroups View in the navigation tree. We have also chosen to view our group with the **Switches** tab.

To create Port Groups, we go to the File pull-down menu and select **Groups** and then select **Edit Port Groups** or alternatively right-click the PortGroups item in the SAN Elements panel. Here we go through the same steps as we did for creating a switch group. When we are done adding a Port Group, we click **OK** to return to the main panel. In Figure 1-148 we show the creation of a Port group.

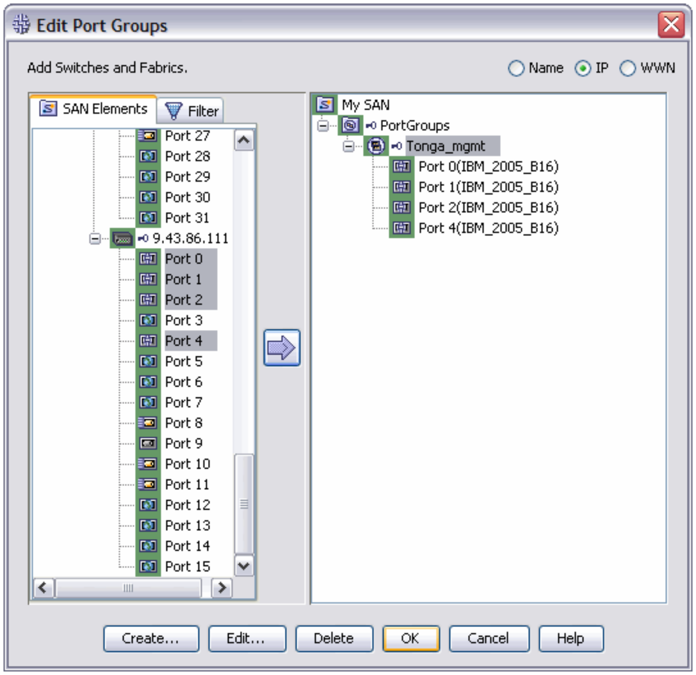
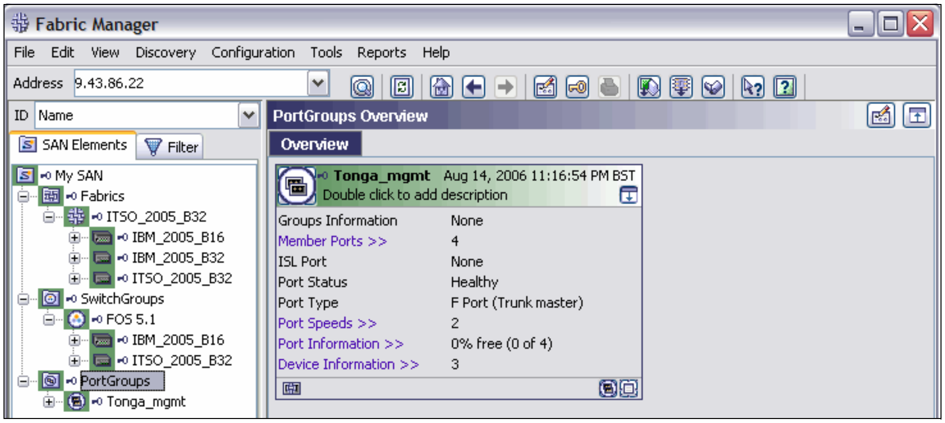

Edit Port Groups
Add Switches and Fabrics.
○ Name ● IP ○ WWN
SAN Elements
Filter
Port 27
Port 28
Port 29
Port 30
Port 31
9.43.86.111
Port 0
Port 1
Port 2
Port 3
Port 4
Port 5
Port 6
Port 7
Port 8
Port 9
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15
My SAN
PortGroups
Tonga_mgmt
Port 0(IBM_2005_B16)
Port 1(IBM_2005_B16)
Port 2(IBM_2005_B16)
Port 4(IBM_2005_B16)
Create...
Edit...
Delete
OK
Cancel
Help

Figure 1-148 Creating a Port group

The newly created port group can now be seen in the Port Groups Overview as detailed in Figure 1-149.


Fabric Manager
File
Edit
View
Discovery
Configuration
Tools
Reports
Help
Address
9.43.86.22
ID
Name
SAN Elements
Filter
My SAN
Fabrics
ITSO_2005_B32
IBM_2005_B16
IBM_2005_B32
ITSO_2005_B32
SwitchGroups
FOS 5.1
IBM_2005_B16
ITSO_2005_B32
PortGroups
Tonga_mgmt
PortGroups Overview
Overview
Tonga_mgmt
Aug 14, 2006 11:16:54 PM BST
Double click to add description

Groups Information	None
Member Ports >>	4
ISL Port	None
Port Status	Healthy
Port Type	F Port (Trunk master)
Port Speeds >>	2
Port Information >>	0% free (0 of 4)
Device Information >>	3

Figure 1-149 Overview of a Port Group

Sharing logical groups definitions

We can export logical group definitions in order to back up our configuration or to share these definitions with another host.

To share logical groups definitions, perform the following steps:

1. Select **File** → **Groups**.
2. Select **Export**.
3. Use the **Browse** button to select a file to Export a Group to.
4. Type a name for your “group” file.
5. Highlight the name of the group(s) to be exported from the navigation-tree.
6. Add the group to be exported by clicking the arrow button, or by dragging and dropping selections from the navigation-tree to the table.
7. Select **Save**.

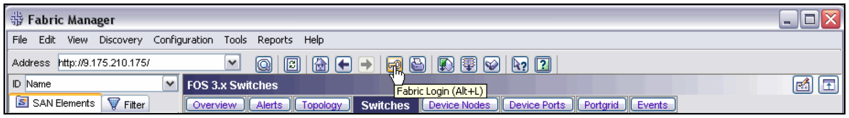
We can now import our group to a separate Fabric Manager machine:

1. Select **File** → **Groups**.
2. Select **Import**.
3. Browse to select the file you previously exported to.

Fabric Login

In order to be able to operate on the switches in the fabric, we have to perform a “Fabric Login”. Fabric Login is necessary, for example, to perform firmware upgrades or a switch reboot.

To define the Fabric Login procedure, click the key icon in the Fabric View as shown in Figure 1-150, which launches the process.


Fabric Manager
File
Edit
View
Discovery
Configuration
Tools
Reports
Help
ID
Name
SAN Elements
Filter
FOS 3.x Switches
Fabric Login (Alt+L)
Overview
Alerts
Topology
Switches
Device Nodes
Device Ports
Portgrid
Events

Address http://9.175.210.175/

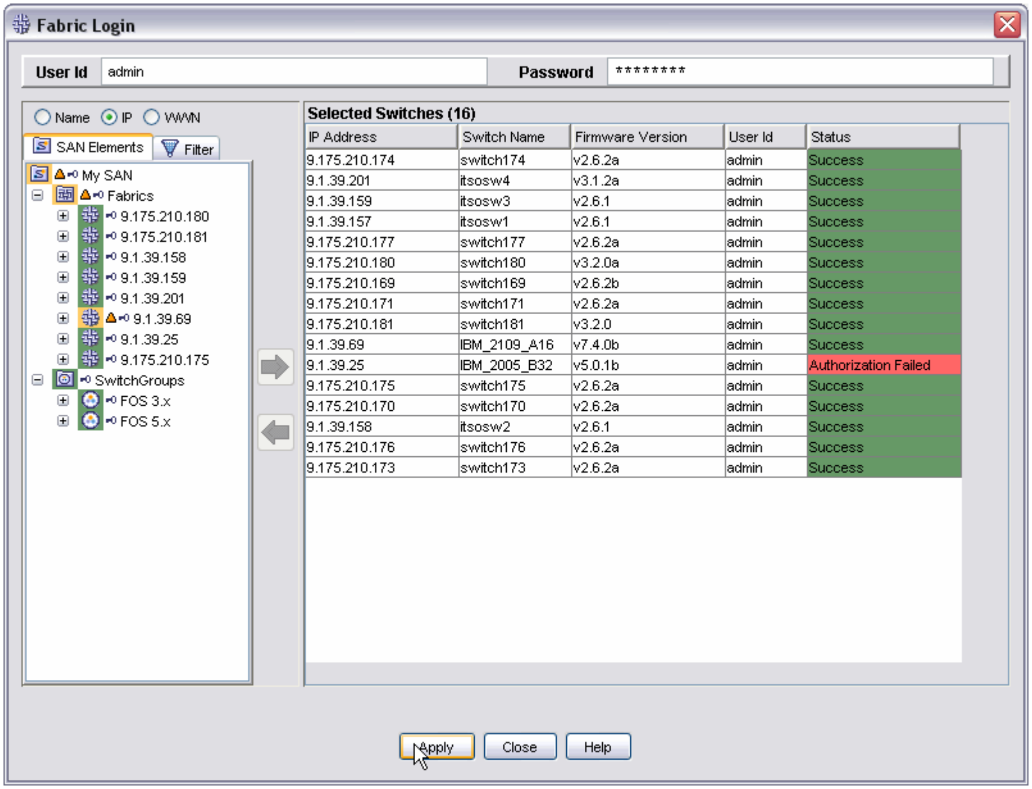
Figure 1-150 Fabric login button

To login to multiple switches:

- From the left-hand side navigation tree, highlight the switches or groups of switches to be selected. (We can select multiple items by holding down the Ctrl key while clicking).
- Use the Add/Delete arrows in the middle column to select the switches.
- The selected switches are applied in a table with all their details.

- Enter the User Name and Password that apply to the switches you selected. This User Name is the same as the one you would use to log into the switch using a Telnet command.
- Choose the **Apply** button to test and apply the login.

Figure 1-55 shows an example of the Fabric Login window. We can see in the status field that authorization failed for one of the switches.



User Id admin

Password ********

Selected Switches (16)

IP Address	Switch Name	Firmware Version	User Id	Status
9.175.210.174	switch174	v2.6.2a	admin	Success
9.1.39.201	itsosw4	v3.1.2a	admin	Success
9.1.39.159	itsosw3	v2.6.1	admin	Success
9.1.39.157	itsosw1	v2.6.1	admin	Success
9.175.210.177	switch177	v2.6.2a	admin	Success
9.175.210.180	switch180	v3.2.0a	admin	Success
9.175.210.169	switch169	v2.6.2b	admin	Success
9.175.210.171	switch171	v2.6.2a	admin	Success
9.175.210.181	switch181	v3.2.0	admin	Success
9.1.39.69	IBM_2109_A16	v7.4.0b	admin	Success
9.1.39.25	IBM_2005_B32	v5.0.1b	admin	Authorization Failed
9.175.210.175	switch175	v2.6.2a	admin	Success
9.175.210.170	switch170	v2.6.2a	admin	Success
9.1.39.158	itsosw2	v2.6.1	admin	Success
9.175.210.176	switch176	v2.6.2a	admin	Success
9.175.210.173	switch173	v2.6.2a	admin	Success

Figure 1-151 Fabric Login

Downloading firmware to multiple switches

Fabric Manager allows you to upgrade firmware on multiple switches without having to log into every single device and run the firmware download process. See “Switch firmware repository” on page 234 for details on how to set up a firmware repository using Fabric Manager.

Prior to downloading firmware to multiple switches, you should make sure that you are logged into the switches you want to upgrade.

We can access the firmware download by clicking the **Download Firmware to switches** icon from the tool bar or alternatively by selecting **Firmware Management** followed by **Firmware Download to Switches** from the Tools menu as detailed in Figure 1-152.

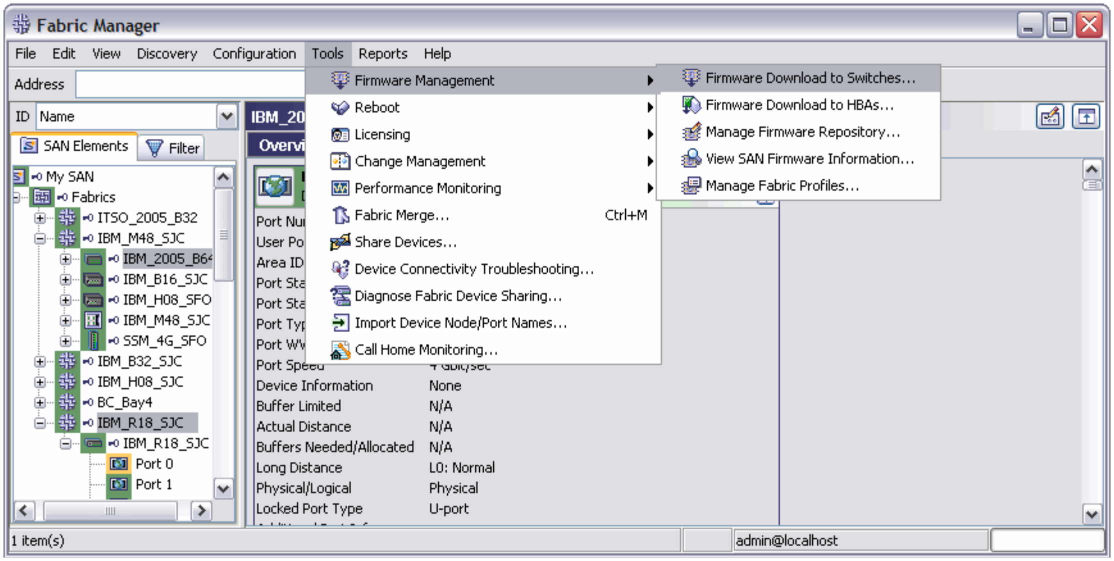
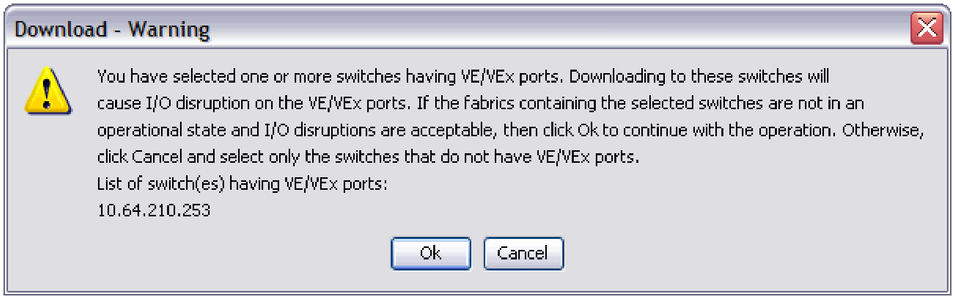

Fabric Manager
File Edit View Discovery Configuration Tools Reports Help
Address
Firmware Management
Reboot
Licensing
Change Management
Performance Monitoring
Fabric Merge... Ctrl+M
Share Devices...
Device Connectivity Troubleshooting...
Diagnose Fabric Device Sharing...
Import Device Node/Port Names...
Call Home Monitoring...
Firmware Download to Switches...
Firmware Download to HBAs...
Manage Firmware Repository...
View SAN Firmware Information...
Manage Fabric Profiles...
ID Name
SAN Elements
Filter
My SAN
Fabrics
ITSO_2005_B32
IBM_M48_SJC
IBM_2005_B64
IBM_B16_SJC
IBM_H08_SFO
IBM_M48_SJC
SSM_4G_SFO
IBM_B32_SJC
IBM_H08_SJC
BC_Bay4
IBM_R18_SJC
IBM_R18_SJC
Port 0
Port 1
Device Information None
Buffer Limited N/A
Actual Distance N/A
Buffers Needed/Allocated N/A
Long Distance L0: Normal
Physical/Logical Physical
Locked Port Type U-port
1 item(s)
admin@localhost

Figure 1-152 Accessing Firmware Download via the Tools menu

Because the IBM_R18_SJC switch we have selected is a router with VE/VEx ports (FCIP link) in place, we are warned that downloading firmware to this switch will cause I/O disruption. During our upgrade this switch was not operational, and as such, we clicked **OK** to continue. See Figure 1-153 for full details of the warning.


Download - Warning

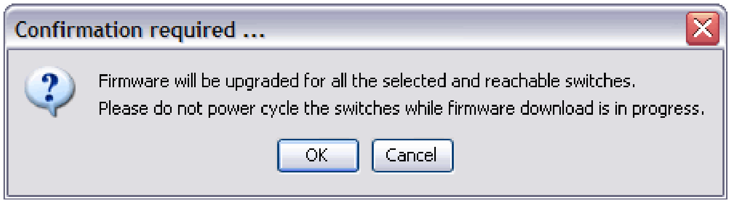
You have selected one or more switches having VE/VEx ports. Downloading to these switches will cause I/O disruption on the VE/VEx ports. If the fabrics containing the selected switches are not in an operational state and I/O disruptions are acceptable, then click Ok to continue with the operation. Otherwise, click Cancel and select only the switches that do not have VE/VEx ports.

List of switch(es) having VE/VEx ports:

10.64.210.253

Figure 1-153 Firmware Download Warning due to VE/VEx ports

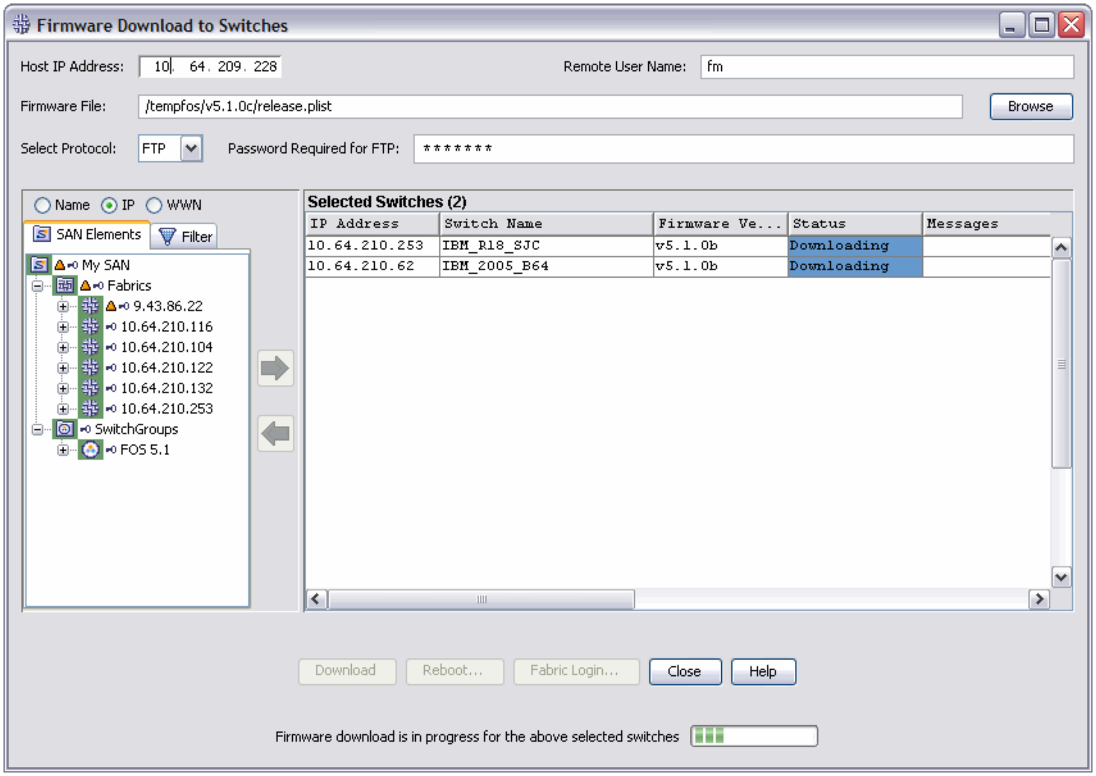
On selecting **OK** it is then necessary to confirm that we want to upgrade the firmware, as detailed in Figure 1-154.


Confirmation required ...
OK
Cancel

Firmware will be upgraded for all the selected and reachable switches.
Please do not power cycle the switches while firmware download is in progress.

Figure 1-154 Confirm firmware upgrade

When we click **OK**, the *Firmware Download to Switches* window detailed in Figure 1-155 appears. We enter the Host IP Address of the FTP server on which the firmware release is available, as well as the user id and password, then click Download to proceed. We can watch the window to monitor the upgrade status to the switches.


Firmware Download to Switches
Browse
○ Name ● IP ○ WWN
SAN Elements
Filter
My SAN
Fabrics
9.43.86.22
10.64.210.116
10.64.210.104
10.64.210.122
10.64.210.132
10.64.210.253
SwitchGroups
FOS 5.1
Download
Reboot...
Fabric Login...
Close
Help

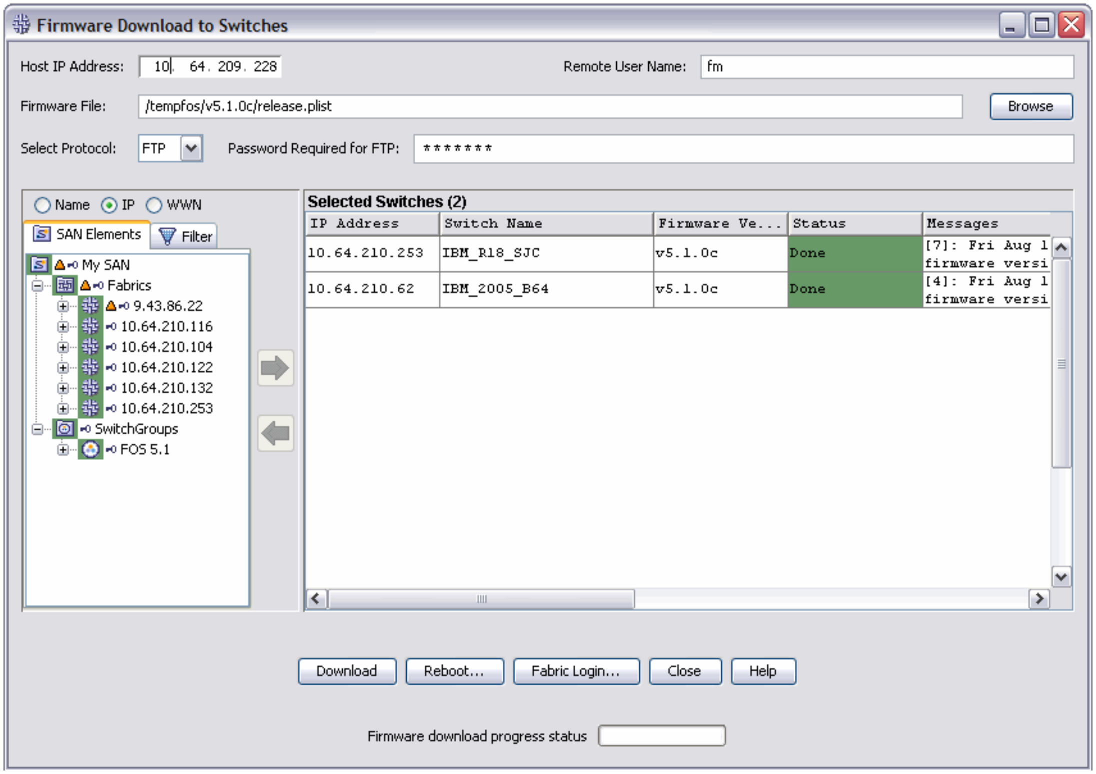
Host IP Address: 10. 64. 209. 228
Remote User Name: fm
Firmware File: /tempfos/v5.1.0c/release.plist
Select Protocol: FTP
Password Required for FTP: *******

Selected Switches (2)

IP Address	Switch Name	Firmware Ve...	Status	Messages
10.64.210.253	IBM_R18_SJC	v5.1.0b	Downloading	
10.64.210.62	IBM_2005_B64	v5.1.0b	Downloading	

Firmware download is in progress for the above selected switches

On completion, the status is highlighted green and states *Done* as seen in Figure 1-155.


Firmware Download to Switches
○ Name ● IP ○ WWN
SAN Elements
Filter
My SAN
Fabrics
9.43.86.22
10.64.210.116
10.64.210.104
10.64.210.122
10.64.210.132
10.64.210.253
SwitchGroups
FOS 5.1
Browse
Download
Reboot...
Fabric Login...
Close
Help
Firmware download progress status

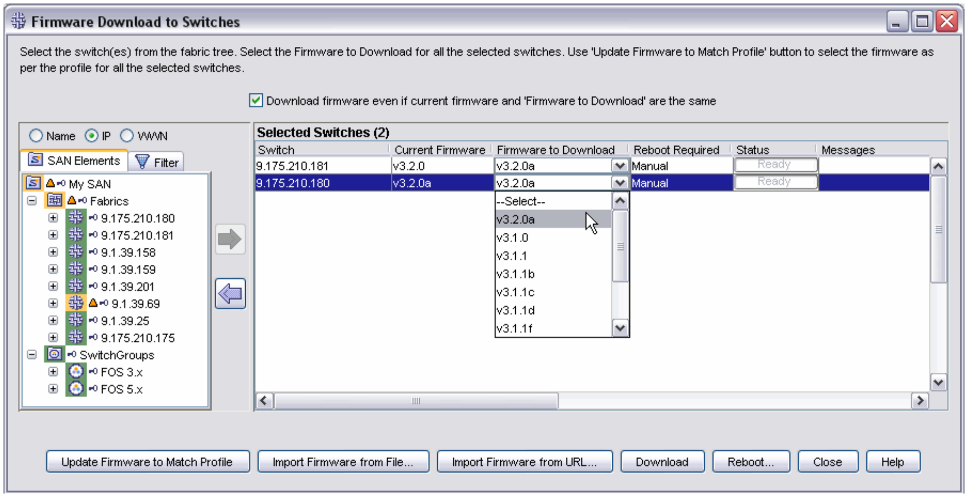
Host IP Address: 10. 64. 209. 228
Remote User Name: fm
Firmware File: /tempfos/v5.1.0c/release.plist
Select Protocol: FTP
Password Required for FTP: *******

Selected Switches (2)

IP Address	Switch Name	Firmware Ve...	Status	Messages
10.64.210.253	IBM_R18_SJC	v5.1.0c	Done	[7]: Fri Aug 1 firmware versi
10.64.210.62	IBM_2005_B64	v5.1.0c	Done	[4]: Fri Aug 1 firmware versi

Figure 1-155 Firmware update to multiple switches complete

The Firmware Download window is then displayed as shown in Figure 1-156.


Firmware Download to Switches
My SAN
Fabrics
9.175.210.180
9.175.210.181
9.1.39.158
9.1.39.159
9.1.39.201
9.1.39.69
9.1.39.25
9.175.210.175
SwitchGroups
FOS 3.x
FOS 5.x
--Select--
v3.2.0a
v3.1.0
v3.1.1
v3.1.1b
v3.1.1c
v3.1.1d
v3.1.1f
Update Firmware to Match Profile
Import Firmware from File...
Import Firmware from URL...
Download
Reboot...
Close
Help

Select the switch(es) from the fabric tree. Select the Firmware to Download for all the selected switches. Use 'Update Firmware to Match Profile' button to select the firmware as per the profile for all the selected switches.

☑ Download firmware even if current firmware and 'Firmware to Download' are the same

○ Name ● IP ○ WWN

SAN Elements | Filter

Selected Switches (2)

Switch	Current Firmware	Firmware to Download	Reboot Required	Status	Messages
9.175.210.181	v3.2.0	v3.2.0a	Manual	Ready	
9.175.210.180	v3.2.0a	v3.2.0a	Manual	Ready	

Figure 1-156 Firmware Download window

To use the Firmware Download window to upgrade the firmware of multiple switches:

- Highlight switches or groups of switches to be targeted for firmware upgrade.
- Use the Select/Deselect arrows in the middle column to move the switches or drag and drop from the navigation window to the table.
- The selected switches are applied in a table with all their details.
- Enter the Host Name or Host IP address.
- Enter the Remote User Name.
- Use the **Browse** button to select a firmware file from the local host.
- Select download protocol (RSHD or FTP).
- If FTP is the chosen protocol, enter the FTP password.
- Choose the **Download** button to begin firmware download.

When the download process is begun, you can check the process status in the status field.

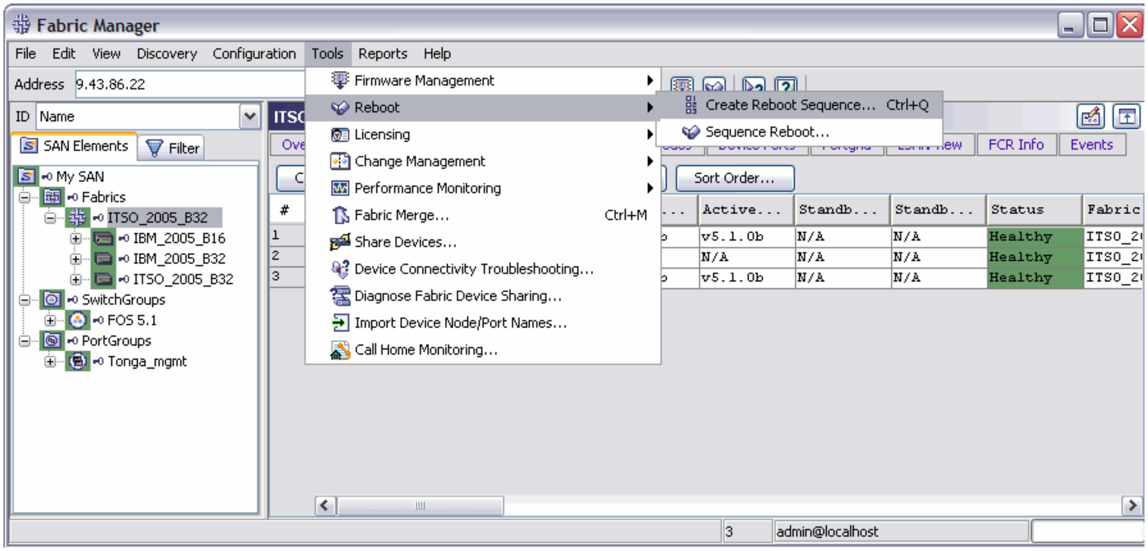
As soon as the firmware download is completed successfully, the Status field turns green. As all switches delivered with FOS 4.1 or later have hot code activation, a reboot is no longer required for the new firmware to take effect.

Sequence Rebooting

Fabric Manager allows you to manage switch reboots and operate on multiple switches at a time.

Create a Reboot Group

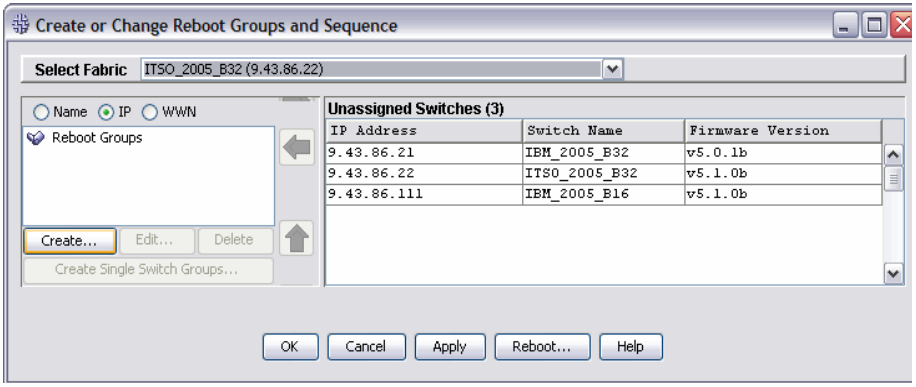
The first step is to create Reboot Groups. To do so, select **Tools** → **Reboot** → **Create Reboot Sequence** as shown in Figure 1-157.


Fabric Manager
File
Edit
View
Discovery
Configuration
Tools
Reports
Help
Address 9.43.86.22
ID Name
SAN Elements
Filter
My SAN
Fabrics
ITSO_2005_B32
IBM_2005_B16
IBM_2005_B32
ITSO_2005_B32
SwitchGroups
FOS 5.1
PortGroups
Tonga_mgmt
Firmware Management
Reboot
Licensing
Change Management
Performance Monitoring
Fabric Merge... Ctrl+M
Share Devices...
Device Connectivity Troubleshooting...
Diagnose Fabric Device Sharing...
Import Device Node/Port Names...
Call Home Monitoring...
Create Reboot Sequence... Ctrl+Q
Sequence Reboot...
FCR Info
Events
Sort Order...
admin@localhost

#	Active...	Standb...	Standb...	Status	Fabric
1	v5.1.0b	N/A	N/A	Healthy	ITSO_2
2	N/A	N/A	N/A	Healthy	ITSO_2
3	v5.1.0b	N/A	N/A	Healthy	ITSO_2

Figure 1-157 Creating a reboot sequence

This displays the window shown Figure 1-158.

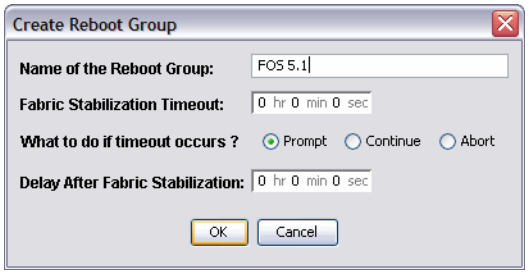

Create or Change Reboot Groups and Sequence
Select Fabric ITSO_2005_B32 (9.43.86.22)
○ Name ● IP ○ WWN
Reboot Groups
Create...
Edit...
Delete
Create Single Switch Groups...
Unassigned Switches (3)
OK
Cancel
Apply
Reboot...
Help

IP Address	Switch Name	Firmware Version
9.43.86.21	IBM_2005_B32	v5.0.1b
9.43.86.22	ITSO_2005_B32	v5.1.0b
9.43.86.111	IBM_2005_B16	v5.1.0b

Figure 1-158 Creating a reboot group

The left hand window displays the created groups. On the right hand side are the switches available in the fabric that we chose from the Select Fabric pulldown list.

To create a reboot group, click the **Create** button. This displays the Create Reboot Group window, where we enter the group name and specify the reboot group options as shown in Figure 1-159.



Create Reboot Group

Name of the Reboot Group: FOS 5.1

Fabric Stabilization Timeout: 0 hr 0 min 0 sec

What to do if timeout occurs ? ● Prompt ○ Continue ○ Abort

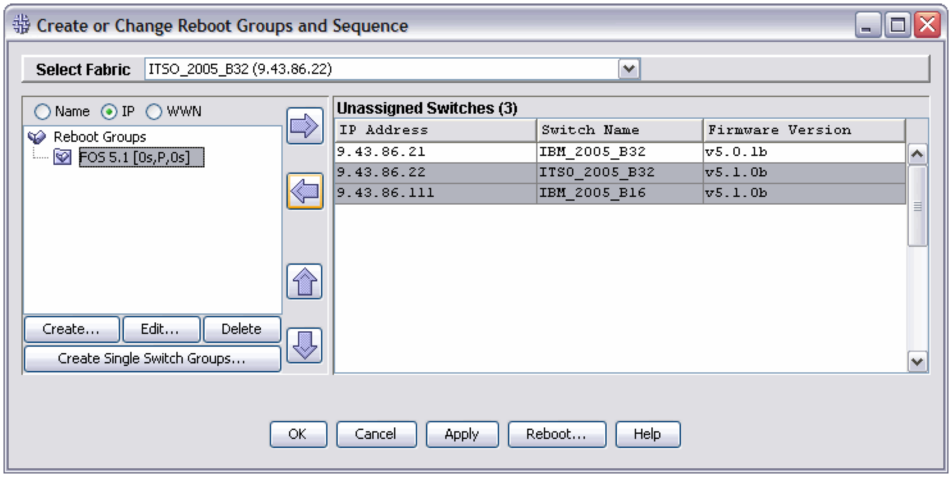
Delay After Fabric Stabilization: 0 hr 0 min 0 sec

Figure 1-159 Create reboot group options window

We click **OK** and return to the main window.

To add switches, we take the following steps shown in Figure 1-160:

1. Highlight the group on the left side list.
2. Highlight the switches to add on the right side list.
3. Click the left **Assign Switches to Reboot Group** arrow.



Create or Change Reboot Groups and Sequence

Select Fabric ITSO_2005_B32 (9.43.86.22)

○ Name ● IP ○ WWN

Reboot Groups
FOS 5.1 [0s,P,0s]

Unassigned Switches (3)

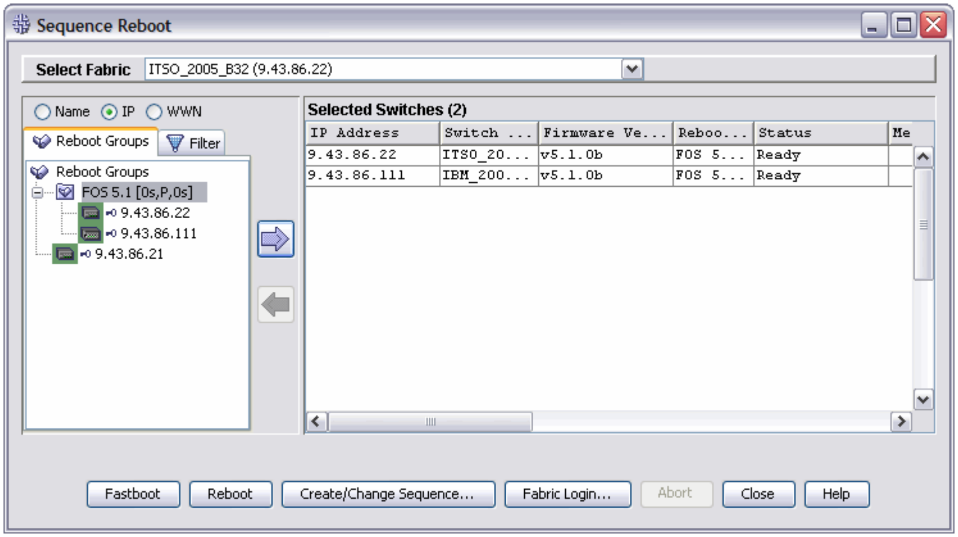
IP Address	Switch Name	Firmware Version
9.43.86.21	IBM_2005_B32	v5.0.1b
9.43.86.22	ITSO_2005_B32	v5.1.0b
9.43.86.111	IBM_2005_B16	v5.1.0b

Figure 1-160 Add switches to reboot group

We now click **Apply** to save or **OK** to save and exit.

Rebooting the switches

To reboot switches, either select **Tools** → **Reboot** → **Sequence Reboot** or click the **Sequence Reboot** button.


Sequence Reboot

Select Fabric: ITSO_2005_B32 (9.43.86.22)

○ Name ● IP ○ WWN

Reboot Groups
Filter
Reboot Groups
FOS 5.1 [0s,P,0s]
9.43.86.22
9.43.86.111
9.43.86.21

Selected Switches (2)

IP Address	Switch ...	Firmware Ve...	Reboo...	Status	Me
9.43.86.22	ITSO_20...	v5.1.0b	FOS 5...	Ready	
9.43.86.111	IBM_200...	v5.1.0b	FOS 5...	Ready	

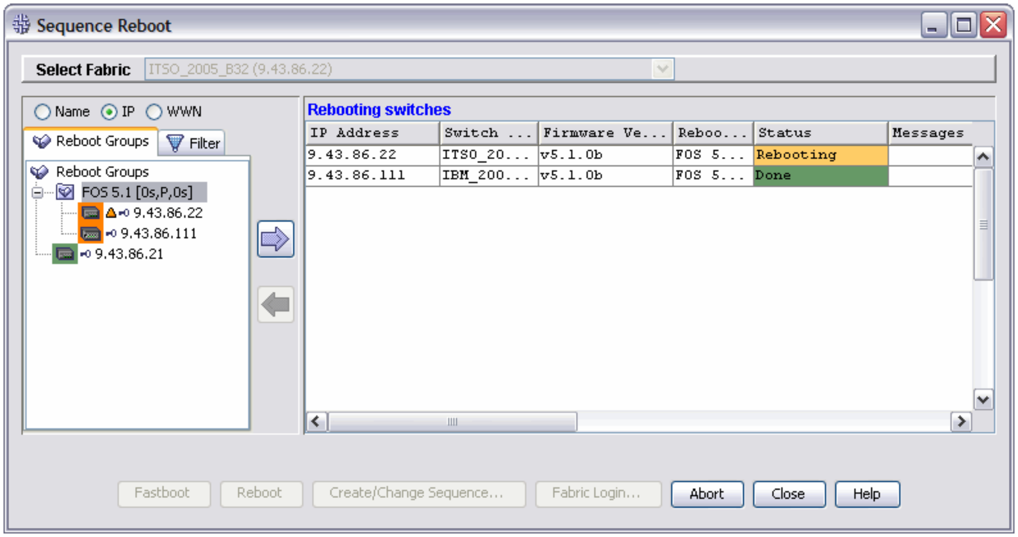
Fastboot
Reboot
Create/Change Sequence...
Fabric Login...
Abort
Close
Help

Figure 1-161 Sequence Reboot window

When the Sequence Reboot window is open, the list on the left hand side displays the Reboot Groups. The list on the right hand side displays the switch(es) selected for reboot.

Highlight a switch or reboot group and then click the **Select Switches** right arrow as shown in Figure 1-162.

Now we select either the **Fastboot** or **Reboot** button to perform the reboot on the selected switches. We can see the switch status of the reboot process in Figure 1-162.


Sequence Reboot
Reboot Groups
Filter
Reboot Groups
FOS 5.1 [0s,P,0s]
9.43.86.22
9.43.86.111
9.43.86.21
Rebooting switches
Fastboot
Reboot
Create/Change Sequence...
Fabric Login...
Abort
Close
Help

Select Fabric: ITSO_2005_B32 (9.43.86.22)

○ Name ● IP ○ WWN

IP Address	Switch ...	Firmware Ve...	Reboo...	Status	Messages
9.43.86.22	ITSO_20...	v5.1.0b	FOS 5...	Rebooting	
9.43.86.111	IBM_200...	v5.1.0b	FOS 5...	Done	

Figure 1-162 Rebooting switches

The switches are rebooted in sequence. In Figure 1-162, the second switch has completed, showing green status and *Done*. The first switch shows yellow status as it is still *Rebooting*.

When the reboot is finished, we receive an Information window notifying us that the reboot sequence is complete; also the “Status” field displays *Done* in green for both switches. We can then click **Close** to exit the window.

Fabric Merge

When merging two different fabrics, conflicts related to zoning, domain ID or operating parameters can occur, causing the new fabric to be segmented.

The Fabric Merge function allows you to check the compatibility of two fabrics before actually merging them.

You can launch “Fabric Merge” by going to **Tools** → **Fabric Merge** as shown in Figure 1-163.

For example, in this section, we work with two fabrics:

- Fabric A with one hub
- Fabric B with two switches

Each of these fabrics has its own set of domain IDs, zoning configurations and operating parameters.

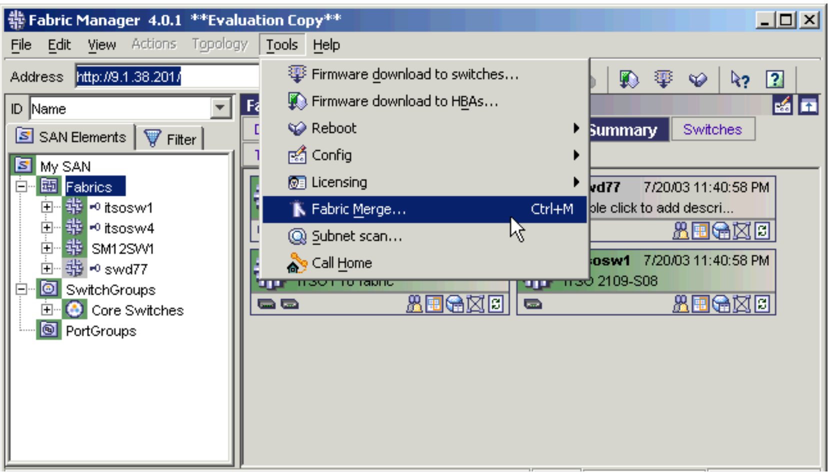

Fabric Manager 4.0.1 **Evaluation Copy**
File Edit View Actions Topology Tools Help
Address http://9.1.38.201/
ID Name
SAN Elements
Filter
My SAN
Fabrics
itsosw1
itsosw4
SM12SW1
swd77
SwitchGroups
Core Switches
PortGroups
Firmware download to switches...
Firmware download to HBAs...
Reboot
Config
Licensing
Fabric Merge... Ctrl+M
Subnet scan...
Call Home
Summary
Switches
7/20/03 11:40:58 PM
2109-S08

Figure 1-163 Launch the Fabric Merge window

The first step is to choose the two fabrics to merge, as shown in Figure 1-164.

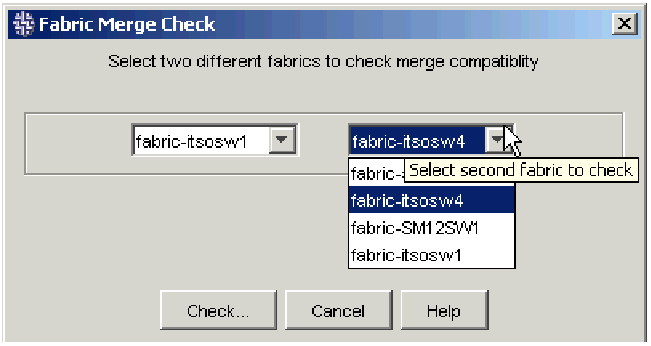
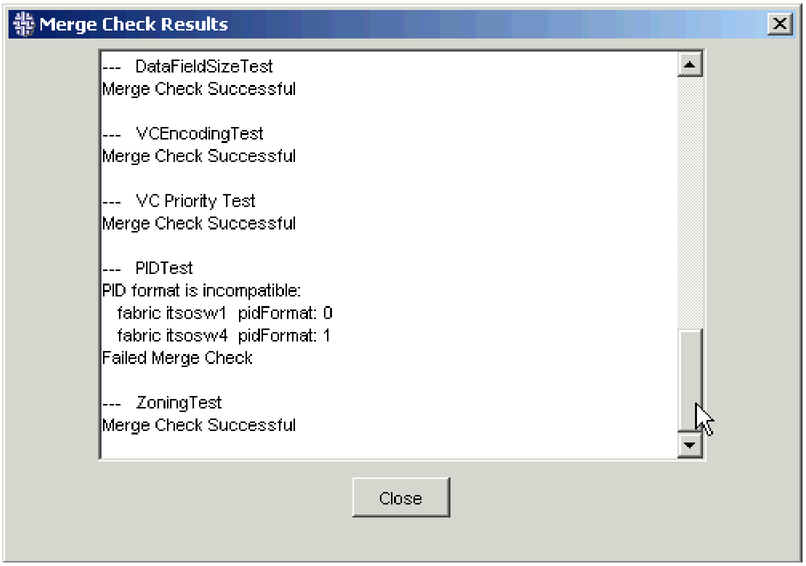

Fabric Merge Check
Select two different fabrics to check merge compatiblity
fabric-itsosw1
fabric-itsosw4
Select second fabric to check
fabric-itsosw4
fabric-SM12SW1
fabric-itsosw1
Check...
Cancel
Help

Figure 1-164 Choose two fabric to merge

For the two fabrics specified here, Fabric Manager downloads the configuration file and checks for any inconsistencies with respect to zoning, domain IDs, and various operating parameters.

When you have clicked the **Check** button, Fabric Manager attempts to connect to each of the fabrics and download their configuration files to the FTP server defined in Figure 1-184.

When the Fabric Manager gets the configuration files, it compares them. In Figure 1-165 we show an example of the parameters not matching, due to core PID not matching.

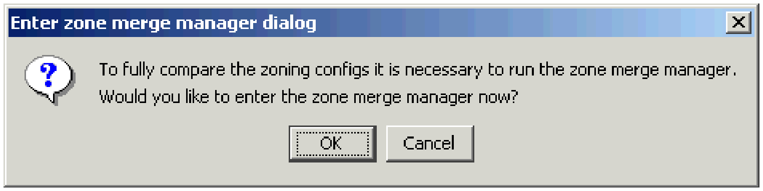


```
---  DataFieldSizeTest
Merge Check Successful

---  VCEncodingTest
Merge Check Successful

---  VC Priority Test
Merge Check Successful

---  PIDTest
PID format is incompatible:
  fabric itsosw1  pidFormat: 0
  fabric itsosw4  pidFormat: 1
Failed Merge Check

---  ZoningTest
Merge Check Successful
```

Figure 1-165   Merge check failure

At this point, we would now close the Merge manager, and manually configure our core PID to match in both fabrics.

If all fabric parameter settings pass the checking, we are then prompted to run the zone merge manager as shown in Figure 1-166.



To fully compare the zoning configs it is necessary to run the zone merge manager. Would you like to enter the zone merge manager now?

Figure 1-166   Zone merge manager prompt

By clicking **OK** we let Fabric Manager help us to resolve conflicts. Fabric manager displays a window as shown in Figure 1-167 with each fabric’s configuration listed.

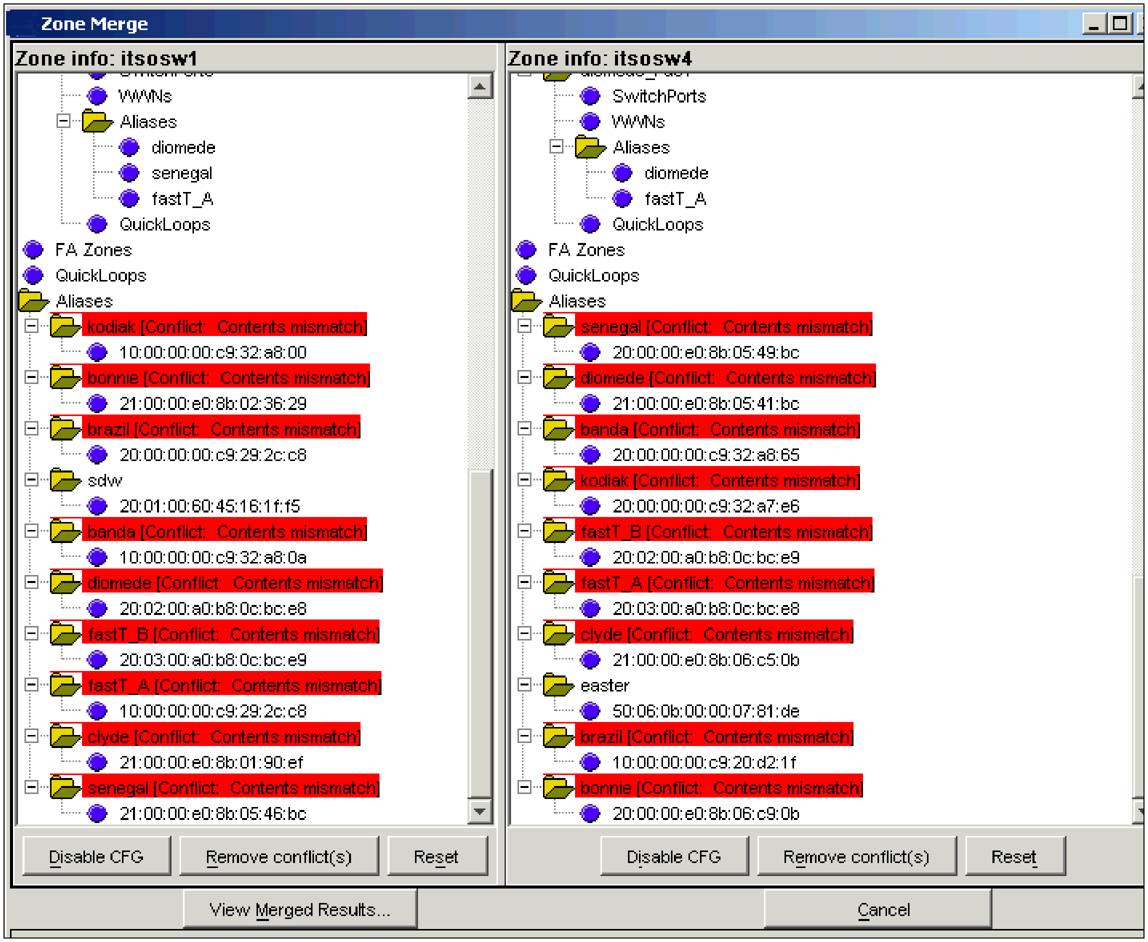

Zone Merge
Zone info: itsosw1
WWNs
Aliases
diomede
senegal
fastT_A
QuickLoops
FA Zones
QuickLoops
Aliases
kodiak [Conflict: Contents mismatch]
10:00:00:00:c9:32:a8:00
bonnie [Conflict: Contents mismatch]
21:00:00:e0:8b:02:36:29
brazil [Conflict: Contents mismatch]
20:00:00:00:c9:29:2c:c8
sdw
20:01:00:60:45:16:1f:f5
banda [Conflict: Contents mismatch]
10:00:00:00:c9:32:a8:0a
diomede [Conflict: Contents mismatch]
20:02:00:a0:b8:0c:bc:e8
fastT_B [Conflict: Contents mismatch]
20:03:00:a0:b8:0c:bc:e9
fastT_A [Conflict: Contents mismatch]
10:00:00:00:c9:29:2c:c8
clyde [Conflict: Contents mismatch]
21:00:00:e0:8b:01:90:ef
senegal [Conflict: Contents mismatch]
21:00:00:e0:8b:05:46:bc
Disable CFG
Remove conflict(s)
Reset
Zone info: itsosw4
SwitchPorts
WWNs
Aliases
diomede
fastT_A
QuickLoops
FA Zones
QuickLoops
Aliases
senegal [Conflict: Contents mismatch]
20:00:00:e0:8b:05:49:bc
diomede [Conflict: Contents mismatch]
21:00:00:e0:8b:05:41:bc
banda [Conflict: Contents mismatch]
20:00:00:00:c9:32:a8:65
kodiak [Conflict: Contents mismatch]
20:00:00:00:c9:32:a7:e6
fastT_B [Conflict: Contents mismatch]
20:02:00:a0:b8:0c:bc:e9
fastT_A [Conflict: Contents mismatch]
20:03:00:a0:b8:0c:bc:e8
clyde [Conflict: Contents mismatch]
21:00:00:e0:8b:06:c5:0b
easter
50:06:0b:00:00:07:81:de
brazil [Conflict: Contents mismatch]
10:00:00:00:c9:20:d2:1f
bonnie [Conflict: Contents mismatch]
20:00:00:e0:8b:06:c9:0b
Disable CFG
Remove conflict(s)
Reset
View Merged Results...
Cancel

Figure 1-167   Zone Merge window

The conflicts are highlighted in red in each configuration tree. In our example, we have conflicts because the configurations both have duplicate alias names.

We can remove the conflicts in one of the fabrics by selecting the conflicts and clicking the **Remove conflict(s)** button. After removing a conflict, we could restore it by clicking the **Reset** button.

In our example, this removes all the aliases for second HBA in each host. This would not be a desirable result, so we cancel the Merge Manager, and alter our aliases on one fabric. Then, when rerunning the Merge Manager, our configurations do not have any conflicts, although the configuration names are highlighted in red, as shown in Figure 1-168.

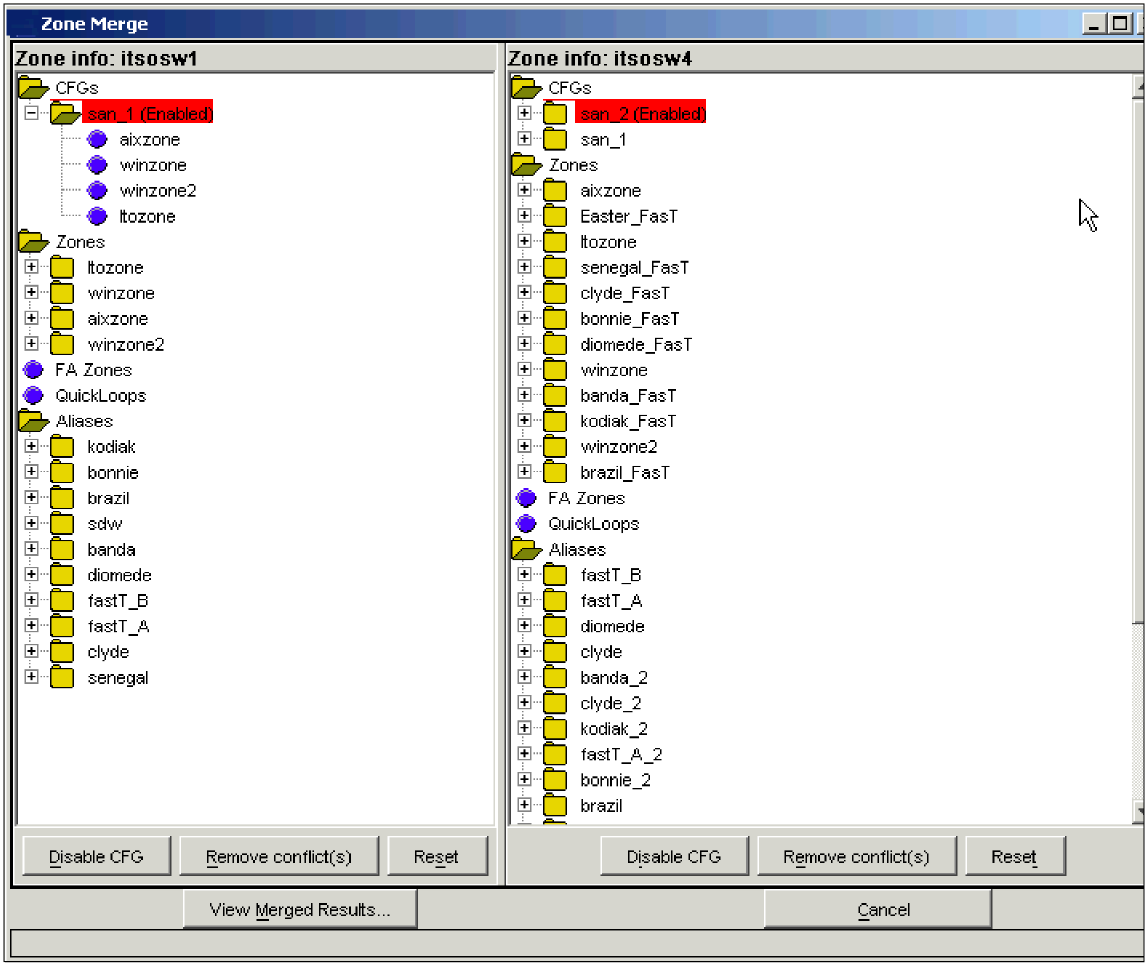

Zone Merge
Zone info: itsosw1
CFGs
san_1 (Enabled)
aixzone
winzone
winzone2
ltozone
Zones
ltozone
winzone
aixzone
winzone2
FA Zones
QuickLoops
Aliases
kodiak
bonnie
brazil
sdw
banda
diomede
fastT_B
fastT_A
clyde
senegal
Disable CFG
Remove conflict(s)
Reset
Zone info: itsosw4
CFGs
san_2 (Enabled)
san_1
Zones
aixzone
Easter_FasT
ltozone
senegal_FasT
clyde_FasT
bonnie_FasT
diomede_FasT
winzone
banda_FasT
kodiak_FasT
winzone2
brazil_FasT
FA Zones
QuickLoops
Aliases
fastT_B
fastT_A
diomede
clyde
banda_2
clyde_2
kodiak_2
fastT_A_2
bonnie_2
brazil
Disable CFG
Remove conflict(s)
Reset
View Merged Results...
Cancel

Figure 1-168 Zone merge conflict removed

Remember when merging zones that only one configuration can be active in a fabric at any one time. As such, we have to disable one of the fabric’s configurations, so that the merge can occur. We use the appropriate **Disable CFG** button to do this.

Now we can click **View Merged Results** to display the final zoning information as shown in Figure 1-169.

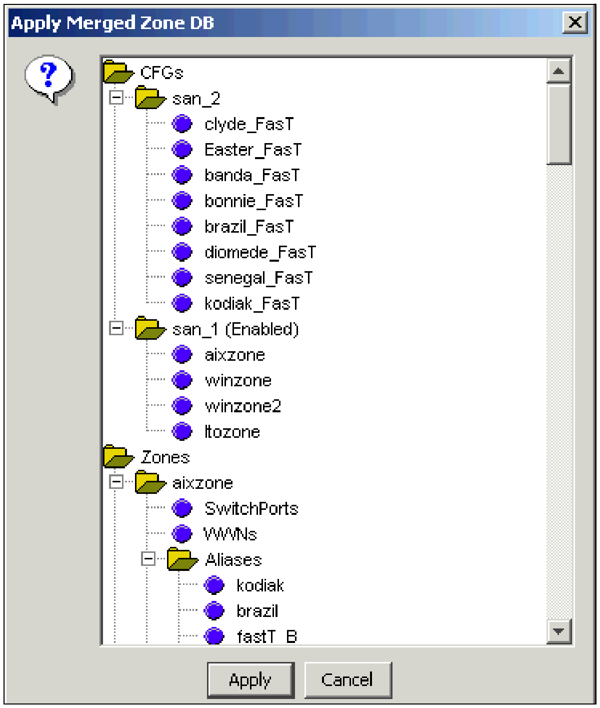

Apply Merged Zone DB
CFGs
san_2
clyde_FasT
Easter_FasT
banda_FasT
bonnie_FasT
brazil_FasT
diomede_FasT
senegal_FasT
kodiak_FasT
san_1 (Enabled)
aixzone
winzone
winzone2
ltozone
Zones
aixzone
SwitchPorts
WWNs
Aliases
kodiak
brazil
fastT_B
Apply
Cancel

Figure 1-169 Merged zone window

From this window we can apply the displayed zoning configuration or cancel to return to the previous window.

Attention: Clicking **Apply** modifies the zoning configuration in both fabrics according to the display shown in Figure 1-169, even if the merge is not completed. In our example, the previously active configuration “SAN_2” in Fabric itsosw4 was disabled.

When these steps have completed, without errors, the two fabrics are ready for merging by connecting a physical ISL between them.

Tip: We can use Fabric Manager’s ability to load configuration parameters to multiple switches to configure a whole fabric without having to logon to every single switch.

Loading switch configuration

Fabric Manager allows you to download switch configuration parameters to a file and upload this configuration or part of it to multiple switches.

This can be used, for example, to set SNMP information or fabric operating parameters to multiple switches without having to set these values on each individual device.

The first step is to save an existing configuration from a switch. This can be done by accessing the switch configuration menu **Configuration** → **Save Baseline** in the Fabric View. This brings up the window shown in Figure 1-170.

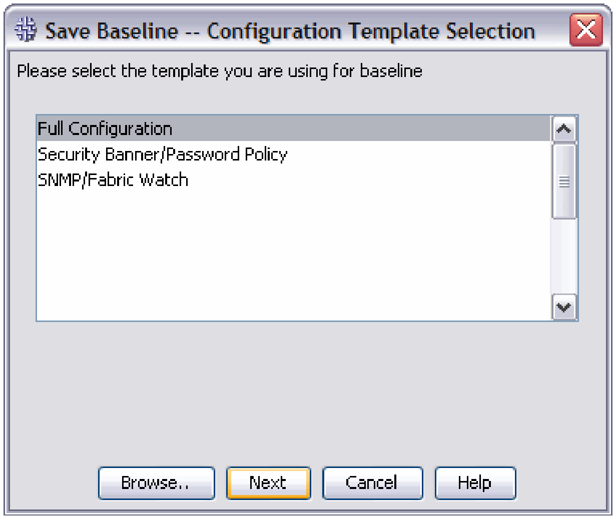

Save Baseline -- Configuration Template Selection
Please select the template you are using for baseline
Full Configuration
Security Banner/Password Policy
SNMP/Fabric Watch
Browse..
Next
Cancel
Help

Figure 1-170 Save Baseline selection window

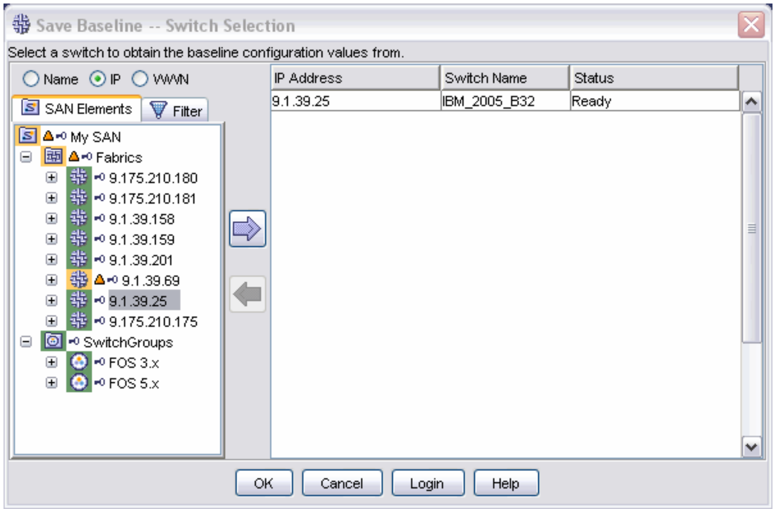
In this window you can select the way in which Fabric Manager presents the configuration parameters:

- **Full Configuration:** This lets you choose from among all the parameters.
- **SNMP/Fabric Watch:** This restricts the selection to SNMP and Fabric Watch parameters only.

In our example, we choose **Full Configuration**.

Selecting one of the above templates enables the **Next** button.

The next step is to choose the switch from which you want to download the configuration, as shown in Figure 1-171.


Save Baseline -- Switch Selection
○ Name ● IP ○ WWN
SAN Elements
Filter
My SAN
Fabrics
9.175.210.180
9.175.210.181
9.1.39.158
9.1.39.159
9.1.39.201
9.1.39.69
9.1.39.25
9.175.210.175
SwitchGroups
FOS 3.x
FOS 5.x
OK
Cancel
Login
Help

Select a switch to obtain the baseline configuration values from.

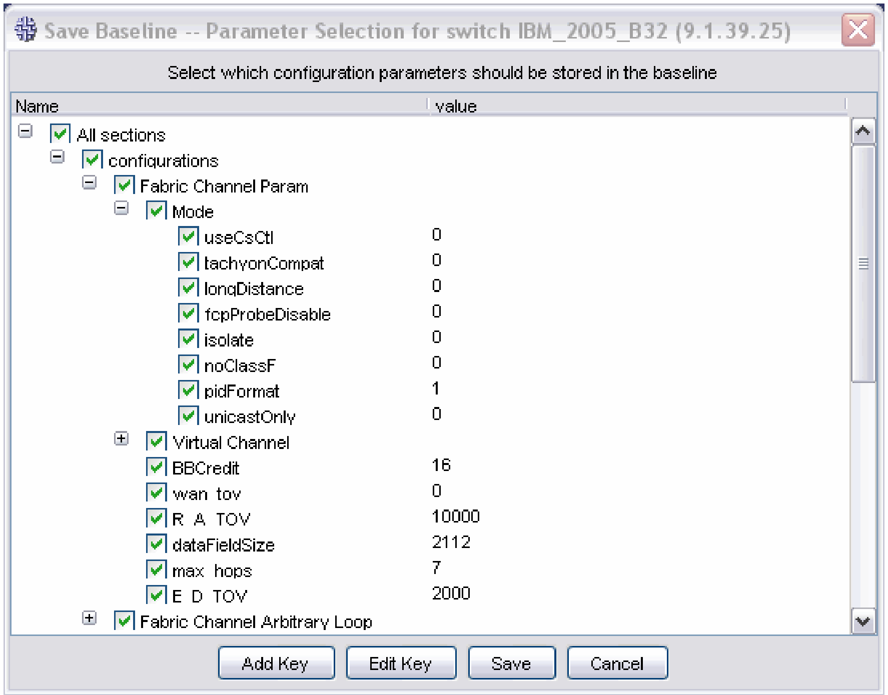
IP Address	Switch Name	Status
9.1.39.25	IBM_2005_B32	Ready

Figure 1-171 Save Baseline — Switch selection

Select the switch from the left-hand list and click the right facing arrow. This adds the switch to the left-hand list. You can download the configuration from only one switch at a time.

You can use the **Login** button to define the log into the switch if it is not already done.

At this time, you should make sure that the FTP server specified in the options is running. Clicking **OK** starts the download of the switch configuration file for file manager internal process. The window shown in Figure 1-172 is displayed.

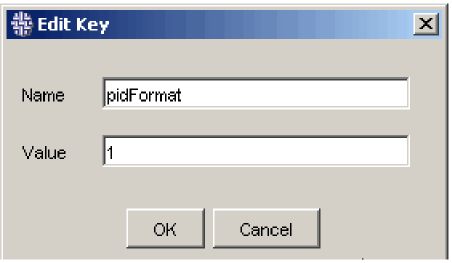

Save Baseline -- Parameter Selection for switch IBM_2005_B32 (9.1.39.25)
Add Key
Edit Key
Save
Cancel

Select which configuration parameters should be stored in the baseline

Name	value
⊟ ☑ All sections	
⊟ ☑ configurations	
⊟ ☑ Fabric Channel Param	
⊟ ☑ Mode	
☑ useCsCtl	0
☑ tachyonCompat	0
☑ longDistance	0
☑ fcpProbeDisable	0
☑ isolate	0
☑ noClassF	0
☑ pidFormat	1
☑ unicastOnly	0
⊞ ☑ Virtual Channel	
☑ BBCredit	16
☑ wan tov	0
☑ R A TOV	10000
☑ dataFieldSize	2112
☑ max hops	7
☑ E D TOV	2000
⊞ ☑ Fabric Channel Arbitrary Loop	

Figure 1-172 Save Baseline — Parameter Selection

From this window, we can choose which parameter or set of parameters we would like to save by checking the corresponding check boxes. In this example, we choose to save only information related to Fabric Parameters. If we would like to change a parameter before saving this Baseline, we can select the *key*, we chose **pidFormat** (the checkbox is slightly greyed), and then clicked the **Edit Key** button, giving us the window shown in Figure 1-173.



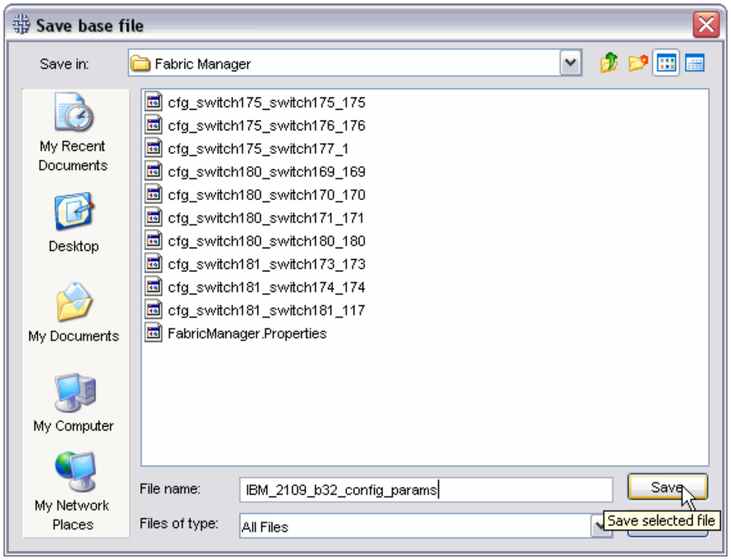
Name: pidFormat

Value: 1

Figure 1-173 Edit parameter key

From the Edit Key window we can change the *Value* field to what we want to be set as our Baseline save.

When we have chosen the parameters to be saved, we click **Save**. This opens a file browsing window where we are able to specify a location for the configuration file, as shown in Figure 1-174.



Save in: Fabric Manager

cfg_switch175_switch175_175
cfg_switch175_switch176_176
cfg_switch175_switch177_1
cfg_switch180_switch169_169
cfg_switch180_switch170_170
cfg_switch180_switch171_171
cfg_switch180_switch180_180
cfg_switch181_switch173_173
cfg_switch181_switch174_174
cfg_switch181_switch181_117
FabricManager.Properties

File name: IBM_2109_b32_config_params

Files of type: All Files

Figure 1-174 Choose a location for configuration file

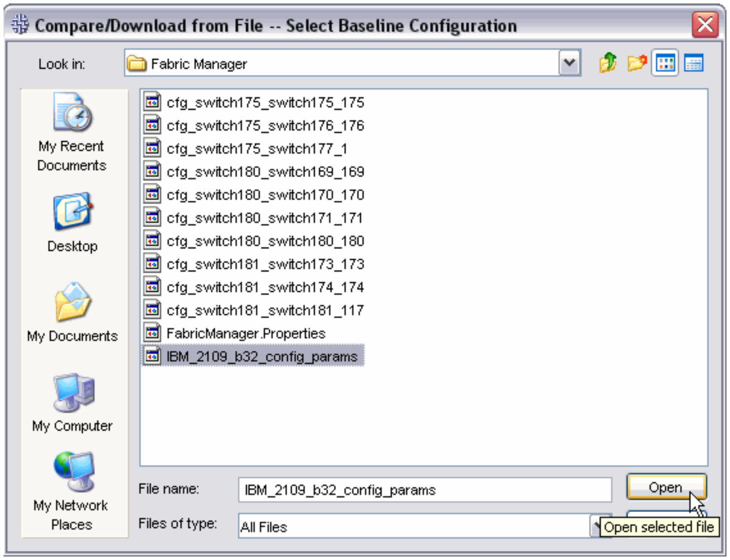
The saved file can now be used to upload the parameters to another switch later on, or can be kept as a backup.

Compare and download file from a file

We can use the file saved in the preceding paragraph to propagate the saved parameters to multiple switches. This can be useful for SNMP information or fabric wide parameters, for example.

Go to **Configuration** → **Compare/Download from File**.

The first step is to choose the file in which configuration parameters are stored. We are prompted to choose a configuration file as shown in Figure 1-175.



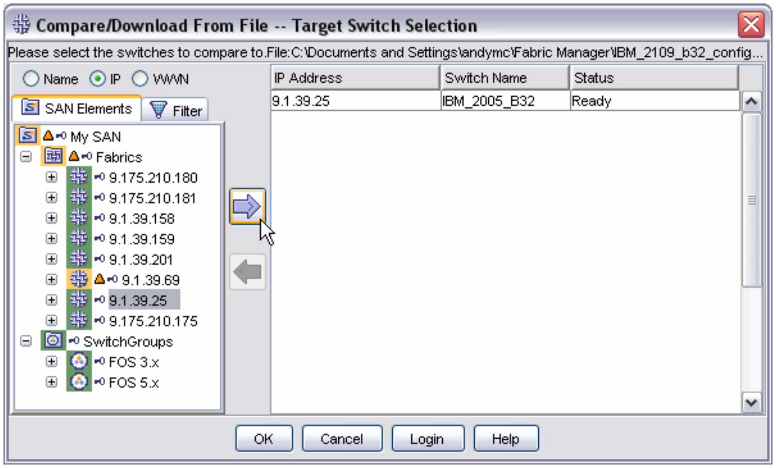
Compare/Download from File -- Select Baseline Configuration
Look in:
Fabric Manager
My Recent Documents
Desktop
My Documents
My Computer
My Network Places
cfg_switch175_switch175_175
cfg_switch175_switch176_176
cfg_switch175_switch177_1
cfg_switch180_switch169_169
cfg_switch180_switch170_170
cfg_switch180_switch171_171
cfg_switch180_switch180_180
cfg_switch181_switch173_173
cfg_switch181_switch174_174
cfg_switch181_switch181_117
FabricManager.Properties
IBM_2109_b32_config_params
Open
Open selected file

File name: IBM_2109_b32_config_params

Files of type: All Files

Figure 1-175 Select configuration file to compare/download

Next, you have to choose the target switches — that is, the switches to which you want to apply the configuration. This is shown in Figure 1-176.



Please select the switches to compare to.File:C:\Documents and Settings\andymc\Fabric Manager\IBM_2109_b32_config...

○ Name ● IP ○ WWN

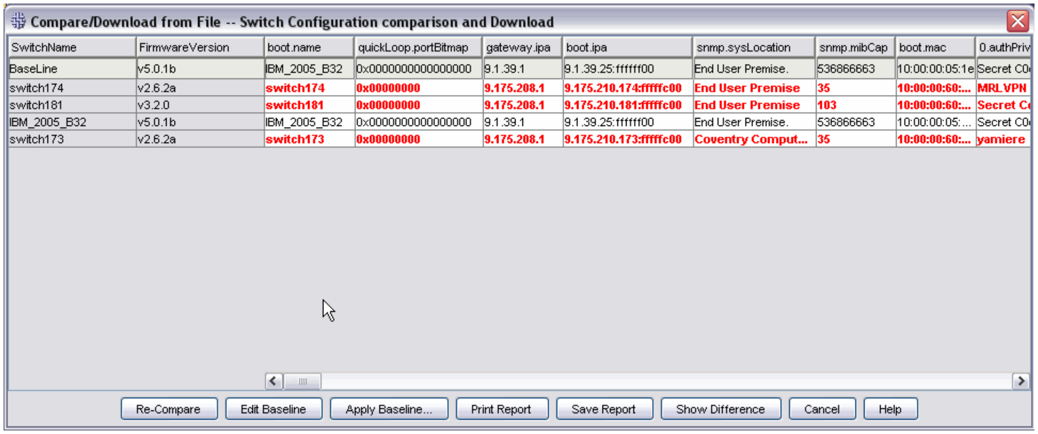
Compare/Download From File -- Target Switch Selection
SAN Elements
Filter
My SAN
Fabrics
9.175.210.180
9.175.210.181
9.1.39.158
9.1.39.159
9.1.39.201
9.1.39.69
9.1.39.25
9.175.210.175
SwitchGroups
FOS 3.x
FOS 5.x
OK
Cancel
Login
Help

IP Address	Switch Name	Status
9.1.39.25	IBM_2005_B32	Ready

Figure 1-176 Compare Download From File — Target Switch Selection

From the left-hand side list, we can select multiple switches. Then click the right facing arrow or drag and drop the selection to the right-hand side list.

Clicking **OK** starts the configuration download from the target switches. Fabric Manager then compares the parameters available in the baseline file to the ones set in the target switch and displays the window shown in Figure 1-177.

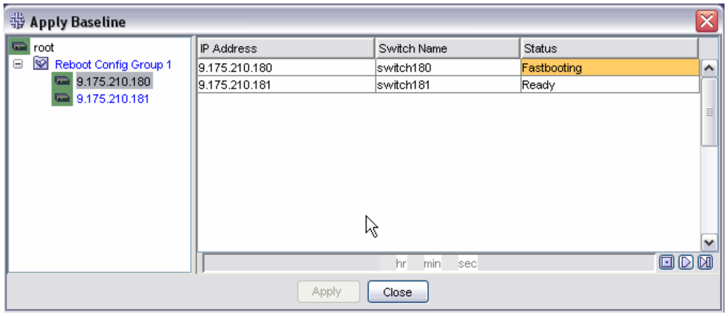

Compare/Download from File -- Switch Configuration comparison and Download
Re-Compare
Edit Baseline
Apply Baseline...
Print Report
Save Report
Show Difference
Cancel
Help

SwitchName	FirmwareVersion	boot.name	quickLoop.portBitmap	gateway.ipa	boot.ipa	snmp.sysLocation	snmp.mibCap	boot.mac	0.authPriv
BaseLine	v5.0.1b	IBM_2005_B32	0x0000000000000000	9.1.39.1	9.1.39.25:ffffff00	End User Premise.	536866663	10:00:00:05:1e	Secret C0
switch174	v2.6.2a	**switch174**	**0x00000000**	**9.175.208.1**	**9.175.210.174:fffffc00**	**End User Premise**	**35**	**10:00:00:60:...**	**MRLVPN**
switch181	v3.2.0	**switch181**	**0x00000000**	**9.175.208.1**	**9.175.210.181:fffffc00**	**End User Premise**	**103**	**10:00:00:60:...**	**Secret C**
IBM_2005_B32	v5.0.1b	IBM_2005_B32	0x0000000000000000	9.1.39.1	9.1.39.25:ffffff00	End User Premise.	536866663	10:00:00:05:...	Secret C0
switch173	v2.6.2a	**switch173**	**0x00000000**	**9.175.208.1**	**9.175.210.173:fffffc00**	**Coventry Comput...**	**35**	**10:00:00:60:...**	**yamiere**

Figure 1-177 Compare/Download from file — Comparison

This window displays in red the differences between the baseline file and the current switches settings. Clicking the **Show Difference** button shows *only* the differences. Then we have the choice to print the comparison report, cancel the operation, edit or apply the baseline, or perform the compare again.

We chose to apply the baseline, so the window in Figure 1-178 is displayed.


Apply Baseline
root
Reboot Config Group 1
9.175.210.180
9.175.210.181
hr
min
sec
Apply
Close

IP Address	Switch Name	Status
9.175.210.180	switch180	Fastbooting
9.175.210.181	switch181	Ready

Figure 1-178 Apply baseline to the switches

Fabric Manager uploads the parameters to each switch, one at a time, and reboot it. As one switch is done (configured and rebooted), it has a strike-through in the switch list in the left-hand side of the window. Notice that you can check the status of the switch being updated in the Status field.

When the baseline is applied to all switches, you can click **Close** to return to the Fabric View.

Managing licenses

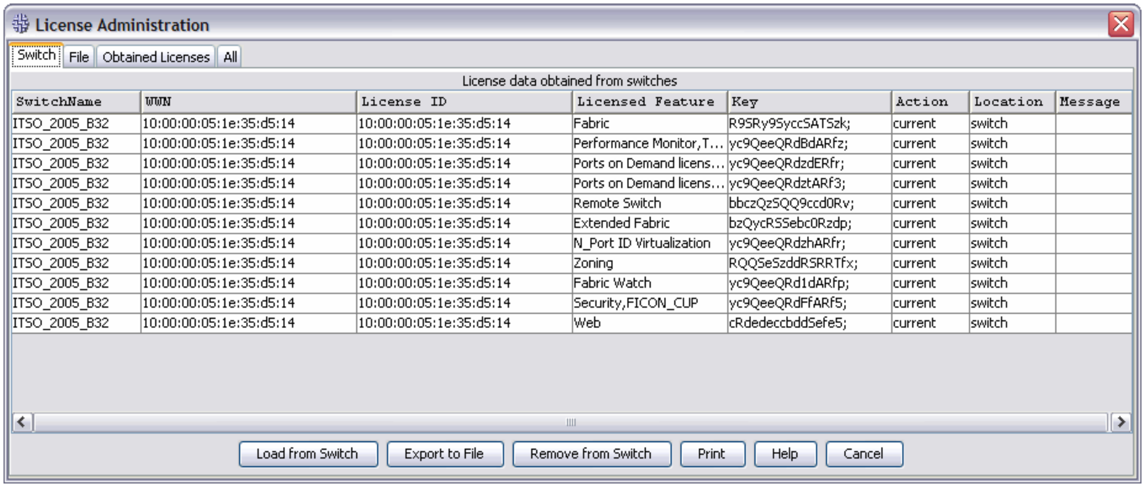
Fabric Manager lets you manage licenses on switches across the fabric. You can:

- View licensing information on each individual switch
- Save licensing information from a switch to a local file for backup
- Download a license file to a switch for upgrade

To manage licensing, go to **Tools** → **Licensing** → **Load from switch**. This displays a switch selection window. Select one or more switches in the left-hand side list and click the right arrow. Validate with **OK**.

Be aware that you have to be logged into the switch. If not, Fabric Manager displays the fabric login window and lets you enter login information.

The License Administration window is shown in Figure 1-179.



License data obtained from switches

SwitchName	WWN	License ID	Licensed Feature	Key	Action	Location	Message
ITSO_2005_B32	10:00:00:05:1e:35:d5:14	10:00:00:05:1e:35:d5:14	Fabric	R9SRy9SyccSATSzk;	current	switch	
ITSO_2005_B32	10:00:00:05:1e:35:d5:14	10:00:00:05:1e:35:d5:14	Performance Monitor,T...	yc9QeeQRdBdARfz;	current	switch	
ITSO_2005_B32	10:00:00:05:1e:35:d5:14	10:00:00:05:1e:35:d5:14	Ports on Demand licens...	yc9QeeQRdzdERfr;	current	switch	
ITSO_2005_B32	10:00:00:05:1e:35:d5:14	10:00:00:05:1e:35:d5:14	Ports on Demand licens...	yc9QeeQRdztARf3;	current	switch	
ITSO_2005_B32	10:00:00:05:1e:35:d5:14	10:00:00:05:1e:35:d5:14	Remote Switch	bbczQzSQQ9ccd0Rv;	current	switch	
ITSO_2005_B32	10:00:00:05:1e:35:d5:14	10:00:00:05:1e:35:d5:14	Extended Fabric	bzQycRSSebc0Rzdp;	current	switch	
ITSO_2005_B32	10:00:00:05:1e:35:d5:14	10:00:00:05:1e:35:d5:14	N_Port ID Virtualization	yc9QeeQRdzhARfr;	current	switch	
ITSO_2005_B32	10:00:00:05:1e:35:d5:14	10:00:00:05:1e:35:d5:14	Zoning	RQQSeSzddRSRRTfx;	current	switch	
ITSO_2005_B32	10:00:00:05:1e:35:d5:14	10:00:00:05:1e:35:d5:14	Fabric Watch	yc9QeeQRd1dARfp;	current	switch	
ITSO_2005_B32	10:00:00:05:1e:35:d5:14	10:00:00:05:1e:35:d5:14	Security,FICON_CUP	yc9QeeQRdFfARf5;	current	switch	
ITSO_2005_B32	10:00:00:05:1e:35:d5:14	10:00:00:05:1e:35:d5:14	Web	cRdedeccbddSefe5;	current	switch	

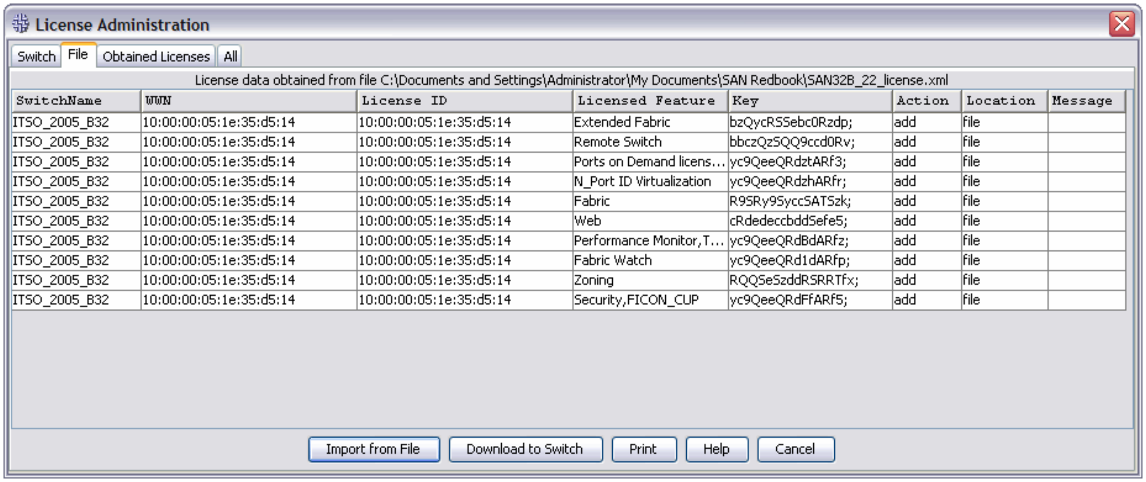
Figure 1-179 License administration — Switch tab

Four tabs are available in this window:

- **Switch:**
  - Lets you view licenses currently installed on the selected switches.
  - Loads licensing information from switches by clicking the **Load from switch** button.
  - Saves the selected license information to an XML file by highlighting the appropriate line(s) and clicking “Export to file”.
  - Lets you view a specific license from the display and remove it, using the “Remove from switch” button.
- **File:**
  - Lets you load licensing information from a saved XML file for display.
  - Lets you select a displayed license and install it to the corresponding switch.
- **Obtained Licenses:**
  - Allows the management and installation of electronically purchased Licenses.
- **All:**
  - Lets you have a consolidated view of all licenses displayed on the other three tabs.

Tip: Do not remove the Web license, because it is required to use Fabric Manager on a switch!

The **File** tab is shown in Figure 1-180.



License data obtained from file C:\Documents and Settings\Administrator\My Documents\SAN Redbook\SAN32B_22_license.xml

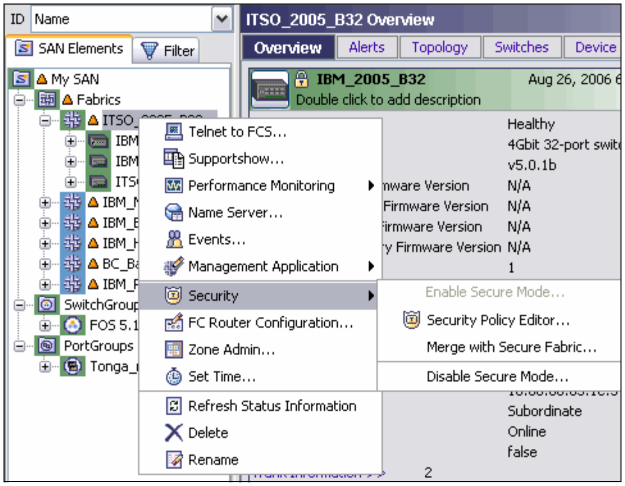
SwitchName	WWN	License ID	Licensed Feature	Key	Action	Location	Message
ITSO_2005_B32	10:00:00:05:1e:35:d5:14	10:00:00:05:1e:35:d5:14	Extended Fabric	bzQycRSSebc0Rzdp;	add	file	
ITSO_2005_B32	10:00:00:05:1e:35:d5:14	10:00:00:05:1e:35:d5:14	Remote Switch	bbczQzSQQ9ccd0Rv;	add	file	
ITSO_2005_B32	10:00:00:05:1e:35:d5:14	10:00:00:05:1e:35:d5:14	Ports on Demand licens…	yc9QeeQRdztARf3;	add	file	
ITSO_2005_B32	10:00:00:05:1e:35:d5:14	10:00:00:05:1e:35:d5:14	N_Port ID Virtualization	yc9QeeQRdzhARfr;	add	file	
ITSO_2005_B32	10:00:00:05:1e:35:d5:14	10:00:00:05:1e:35:d5:14	Fabric	R9SRy9SyccSATSzk;	add	file	
ITSO_2005_B32	10:00:00:05:1e:35:d5:14	10:00:00:05:1e:35:d5:14	Web	cRdedeccbddSefe5;	add	file	
ITSO_2005_B32	10:00:00:05:1e:35:d5:14	10:00:00:05:1e:35:d5:14	Performance Monitor,T…	yc9QeeQRdBdARfz;	add	file	
ITSO_2005_B32	10:00:00:05:1e:35:d5:14	10:00:00:05:1e:35:d5:14	Fabric Watch	yc9QeeQRd1dARfp;	add	file	
ITSO_2005_B32	10:00:00:05:1e:35:d5:14	10:00:00:05:1e:35:d5:14	Zoning	RQQSeSzddRSRRTfx;	add	file	
ITSO_2005_B32	10:00:00:05:1e:35:d5:14	10:00:00:05:1e:35:d5:14	Security,FICON_CUP	yc9QeeQRdFfARf5;	add	file	

Figure 1-180 License Administration — File tab

Security

After enabling an Advanced Security fabric as discussed in “Enabling Advanced Security” on page 287, we are able to manage the security policies from Fabric Manager.

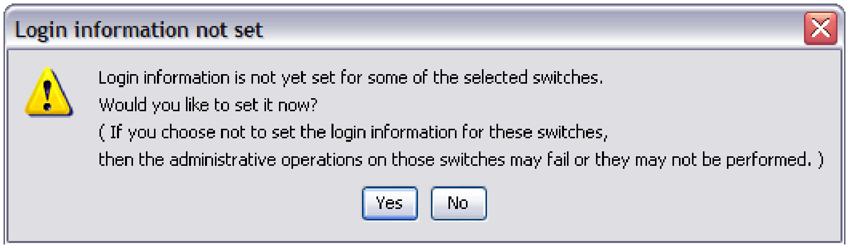
By right-clicking our fabric icon, we launch a menu as shown in Figure 1-181, where we select the **Security...** option.



ITSO_2005_B32 Overview
Overview
Alerts
Topology
Switches
Device
SAN Elements
Filter
My SAN
Fabrics
IBM_2005_B32
Double click to add description
Telnet to FCS...
Supportshow...
Performance Monitoring
Name Server...
Events...
Management Application
Security
FC Router Configuration...
Zone Admin...
Set Time...
Refresh Status Information
Delete
Rename
Enable Secure Mode...
Security Policy Editor...
Merge with Secure Fabric...
Disable Secure Mode...

Figure 1-181 Selecting Security management

When we do this, we receive a message as shown in Figure 1-182 indicating that passwords have not been learned. Although Fabric Manager previously had been defined with passwords for this fabric, during the enabling of Advanced Security, we were forced to change all the passwords.

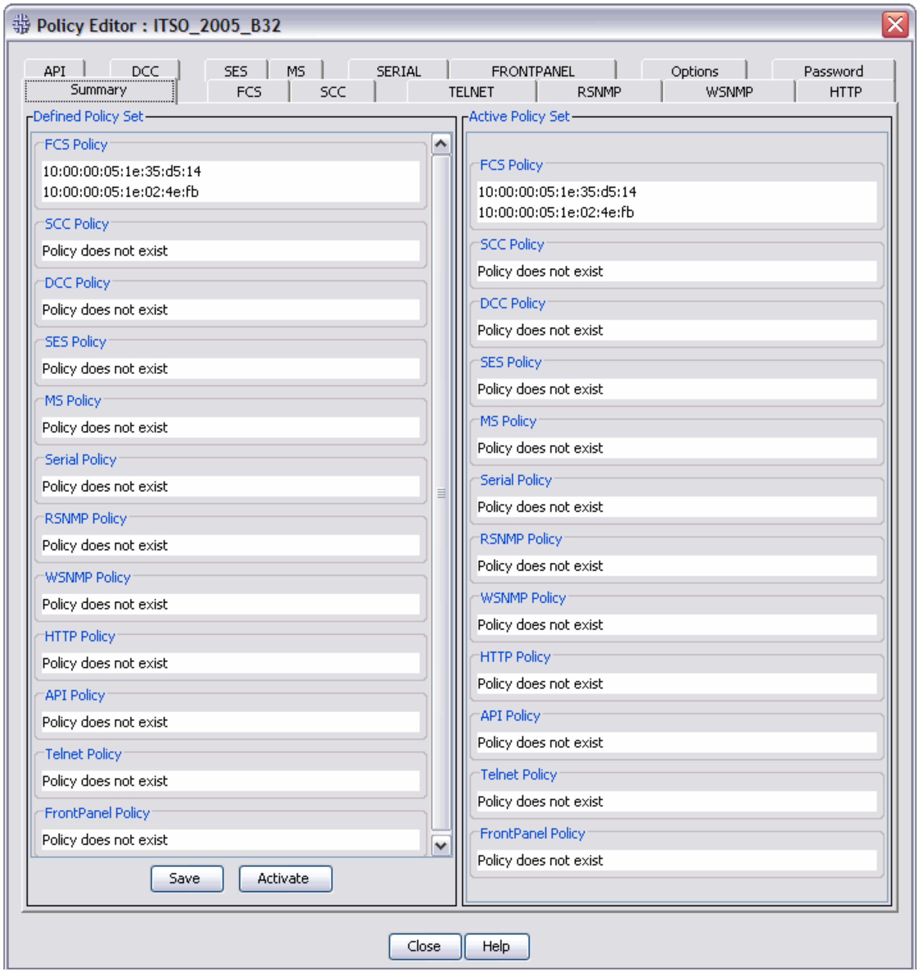


Login information not set

Login information is not yet set for some of the selected switches.
Would you like to set it now?
(If you choose not to set the login information for these switches,
then the administrative operations on those switches may fail or they may not be performed.)

Figure 1-182 Password error message

We answer **Yes** to the message and re-define the passwords as defined in our enabling Security section. When the passwords have been successfully learned, the Security Administration window opens, as shown in Figure 1-183.



Defined Policy Set

FCS Policy
10:00:00:05:1e:35:d5:14
10:00:00:05:1e:02:4e:fb

SCC Policy
Policy does not exist

DCC Policy
Policy does not exist

SES Policy
Policy does not exist

MS Policy
Policy does not exist

Serial Policy
Policy does not exist

RSNMP Policy
Policy does not exist

WSNMP Policy
Policy does not exist

HTTP Policy
Policy does not exist

API Policy
Policy does not exist

Telnet Policy
Policy does not exist

FrontPanel Policy
Policy does not exist

Active Policy Set

FCS Policy
10:00:00:05:1e:35:d5:14
10:00:00:05:1e:02:4e:fb

SCC Policy
Policy does not exist

DCC Policy
Policy does not exist

SES Policy
Policy does not exist

MS Policy
Policy does not exist

Serial Policy
Policy does not exist

RSNMP Policy
Policy does not exist

WSNMP Policy
Policy does not exist

HTTP Policy
Policy does not exist

API Policy
Policy does not exist

Telnet Policy
Policy does not exist

FrontPanel Policy
Policy does not exist

Figure 1-183 Security Policy management

From this window we can view the various security policies, and define them by clicking the appropriate tab on the left side of the window.

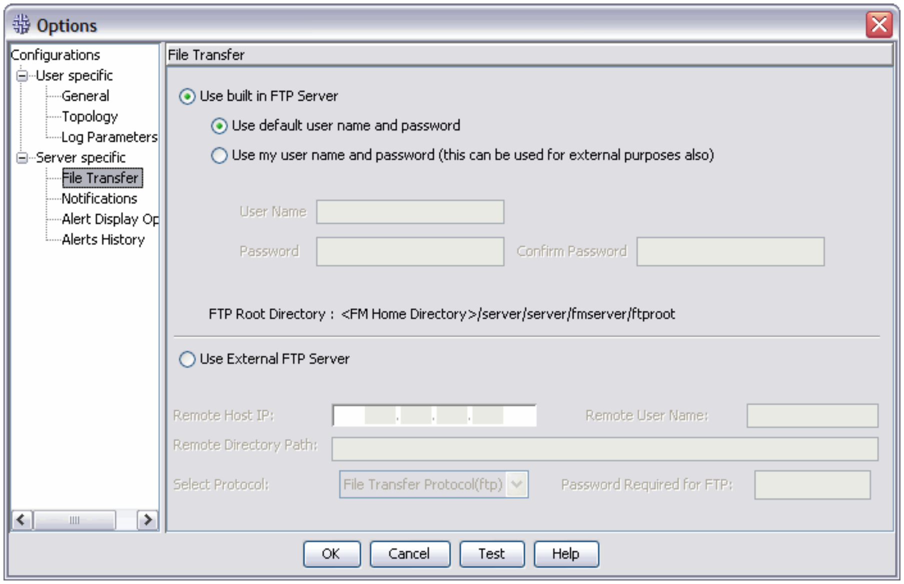
New features found in Fabric Manager 5.x

In the following section we show how to set up and use some of the features introduced in Fabric Manager version 5.0.

Switch firmware repository

The switch firmware repository allows simple storage and maintenance of multiple copies of switch/director firmware and their associated Release Notes. The switches and directors can access the repository during a firmware upgrade or downgrade via the built-in FTP server within Fabric Manager v5.0 and above.

Before we begin to add firmware files into the repository, we must configure the FTP server via the drop-down menu, **Configuration** → **FM options**, as seen in Figure 1-184.


Options
Configurations
User specific
General
Topology
Log Parameters
Server specific
File Transfer
Notifications
Alert Display Op
Alerts History
OK
Cancel
Test
Help

File Transfer

● Use built in FTP Server

● Use default user name and password

○ Use my user name and password (this can be used for external purposes also)

User Name

Password

Confirm Password

FTP Root Directory : <FM Home Directory>/server/server/fmserver/ftproot

○ Use External FTP Server

Remote Host IP:

Remote User Name:

Remote Directory Path:

Select Protocol: File Transfer Protocol(ftp)

Password Required for FTP:

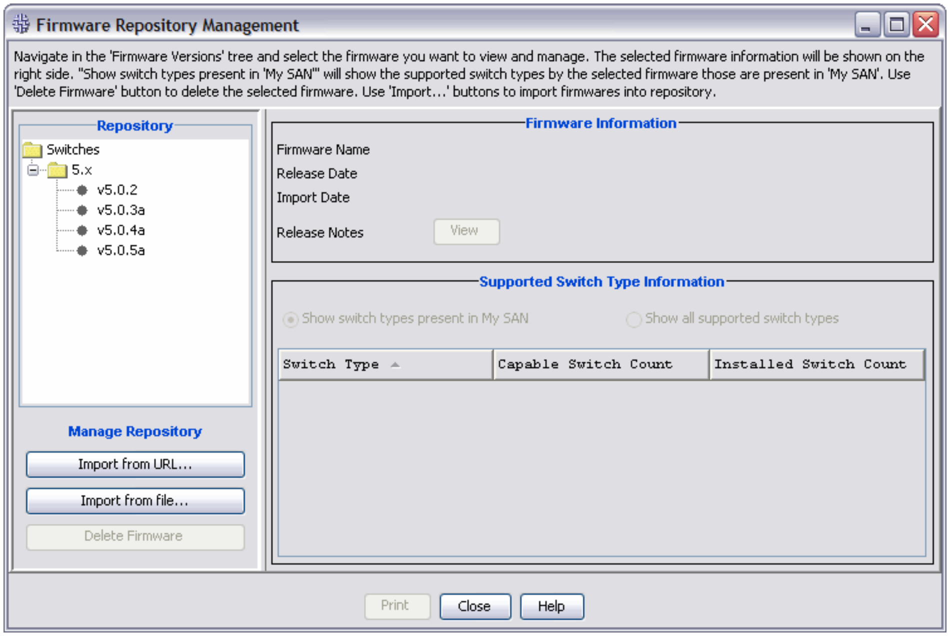
Figure 1-184 Configuration panel for FM internal/external FTP service

From here we can also click the **Test** button to confirm that the FTP server is functioning.

Now that the FTP service is configured and tested, we can start to load firmware files into the repository using the drop-down menu tree, **Tools** → **Firmware Management** → **Manage Firmware Repository**.

Note: You might have to make changes to your firewall configuration in order to implement the firmware repository.

From the newly opened Firmware Repository Management window (see Figure 1-185), we can see that several firmware versions have previously been uploaded into the repository.

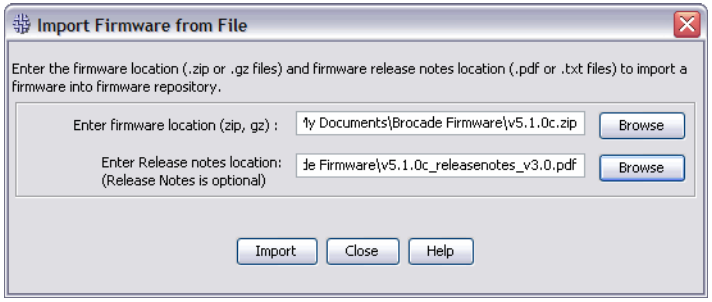


Navigate in the 'Firmware Versions' tree and select the firmware you want to view and manage. The selected firmware information will be shown on the right side. "Show switch types present in 'My SAN'" will show the supported switch types by the selected firmware those are present in 'My SAN'. Use 'Delete Firmware' button to delete the selected firmware. Use 'Import...' buttons to import firmwares into repository.

Firmware Repository Management
Repository
Switches
5.x
v5.0.2
v5.0.3a
v5.0.4a
v5.0.5a
Manage Repository
Import from URL...
Import from file...
Delete Firmware
Firmware Information
Firmware Name
Release Date
Import Date
Release Notes
View
Supported Switch Type Information
● Show switch types present in My SAN
○ Show all supported switch types
Switch Type
Capable Switch Count
Installed Switch Count
Print
Close
Help

Figure 1-185 Firmware Repository Management window

Here, we select the import from file button and populate the text boxes with the appropriate information, as shown in Figure 1-186.



Enter the firmware location (.zip or .gz files) and firmware release notes location (.pdf or .txt files) to import a firmware into firmware repository.

Enter firmware location (zip, gz) : ly Documents\Brocade Firmware\v5.1.0c.zip

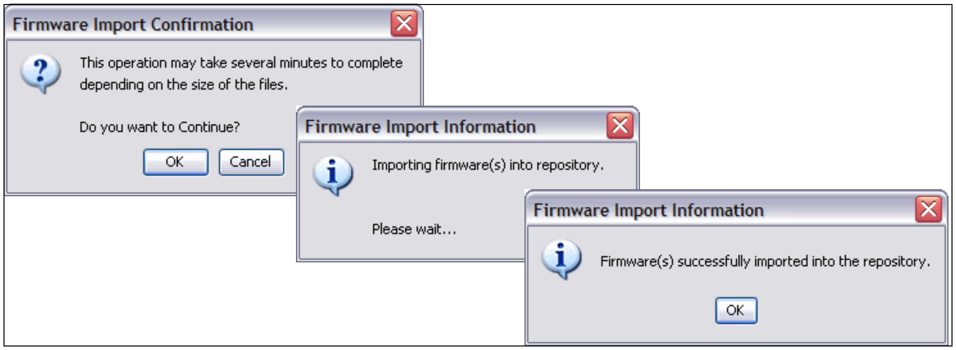
Enter Release notes location: de Firmware\v5.1.0c_releasenotes_v3.0.pdf
(Release Notes is optional)

Import Firmware from File
Browse
Browse
Import
Close
Help

Figure 1-186 Import Firmware from File window

As you can see, we are preparing to upload FOS 5.1.0c and its Release Notes into the repository.

On clicking **Import**, we see a pop-up box warning (Figure 1-187) saying that this process might take a few minutes. This is because the zip/gz files are exploded into the firmware tree. In the case of FOS 5.x, where the firmware file can be over 100 Mb in size, this operation indeed takes a few moments.


Firmware Import Confirmation
OK
Cancel
Firmware Import Information
Firmware Import Information
OK

This operation may take several minutes to complete depending on the size of the files.

Do you want to Continue?

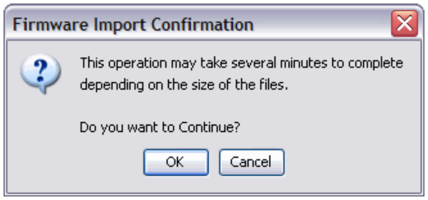
Importing firmware(s) into repository.

Please wait...

Firmware(s) successfully imported into the repository.

Figure 1-187 Firmware Import

The confirmation window is shown in Figure 1-188.

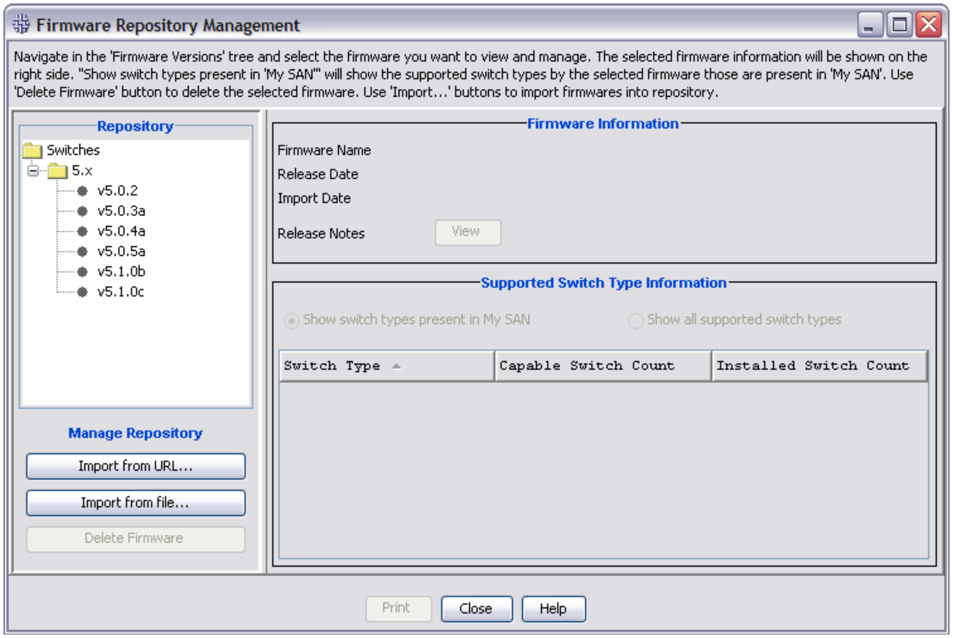

Firmware Import Confirmation
OK
Cancel

This operation may take several minutes to complete depending on the size of the files.

Do you want to Continue?

Figure 1-188 Firmware Import Confirmation Window

After the import has completed, another pop-up box warns us that it will automatically refresh the display, enabling us to see the new code loaded into the repository (Figure 1-189).


Firmware Repository Management
Repository
Switches
5.x
v5.0.2
v5.0.3a
v5.0.4a
v5.0.5a
v5.1.0b
v5.1.0c
Manage Repository
Import from URL...
Import from file...
Delete Firmware
Firmware Information
Firmware Name
Release Date
Import Date
Release Notes
View
Supported Switch Type Information
● Show switch types present in My SAN
○ Show all supported switch types
Switch Type
Capable Switch Count
Installed Switch Count
Print
Close
Help

Navigate in the 'Firmware Versions' tree and select the firmware you want to view and manage. The selected firmware information will be shown on the right side. "Show switch types present in 'My SAN'" will show the supported switch types by the selected firmware those are present in 'My SAN'. Use 'Delete Firmware' button to delete the selected firmware. Use 'Import...' buttons to import firmwares into repository.

Figure 1-189 Firmware Repository window showing newly loaded FOS 5.x code

This process is now complete, as seen in Figure 1-189. Appropriate switches and directors can now connect to the Fabric Manager internal FTP service and download FOS 5.x.

Call home

Now we set up the call home function from FM 5.x. Call Home allows you to monitor the switches for the following four events: A switch status changing from healthy to either a degraded or down status; a switch status remaining either marginal or down but the reason code changing; a switch rebooting; or FM losing connection with a switch. When one of these events is triggered, Call Home sends an e-mail to a number of pre-defined recipients.

Choosing **Configuration** → **Call home** opens up a current status window for this feature, as shown in Figure 1-190. Here we can see that no configuration exists at the moment.

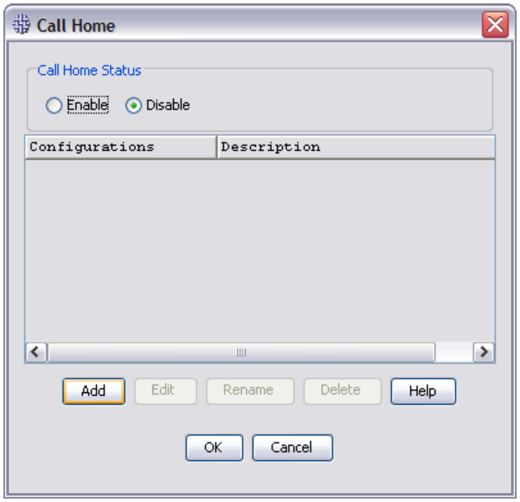
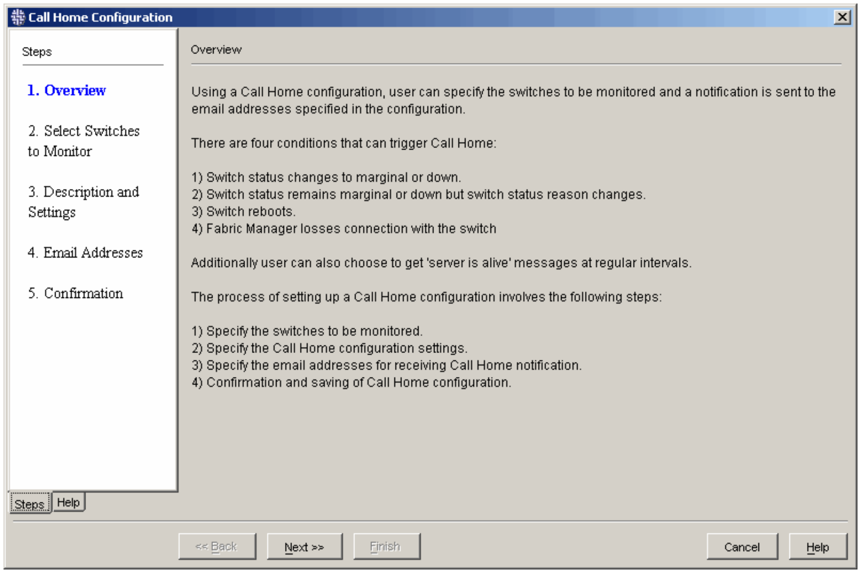

Call Home
Call Home Status
○ Enable ● Disable
Configurations
Description
Add
Edit
Rename
Delete
Help
OK
Cancel

Figure 1-190 Current Call Home status

Clicking the **Add** button spawns the Call Home Configuration wizard, as seen in Figure 1-191.


Call Home Configuration
Steps
1. Overview
2. Select Switches to Monitor
3. Description and Settings
4. Email Addresses
5. Confirmation
Steps
Help
Overview
<< Back
Next >>
Finish
Cancel
Help

Using a Call Home configuration, user can specify the switches to be monitored and a notification is sent to the email addresses specified in the configuration.

There are four conditions that can trigger Call Home:

1) Switch status changes to marginal or down.
2) Switch status remains marginal or down but switch status reason changes.
3) Switch reboots.
4) Fabric Manager losses connection with the switch

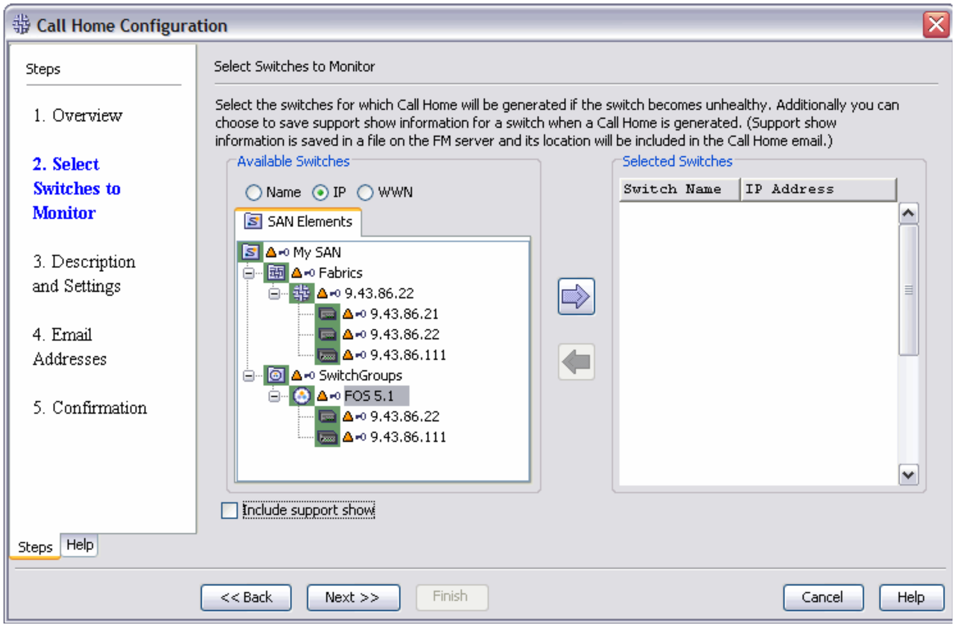
Additionally user can also choose to get 'server is alive' messages at regular intervals.

The process of setting up a Call Home configuration involves the following steps:

1) Specify the switches to be monitored.
2) Specify the Call Home configuration settings.
3) Specify the email addresses for receiving Call Home notification.
4) Confirmation and saving of Call Home configuration.

Figure 1-191 Startup panel for call home wizard

In Figure 1-192 a list of available switches is presented in the left-hand Available Switches box. These can be sorted in IP address order or WWN order.

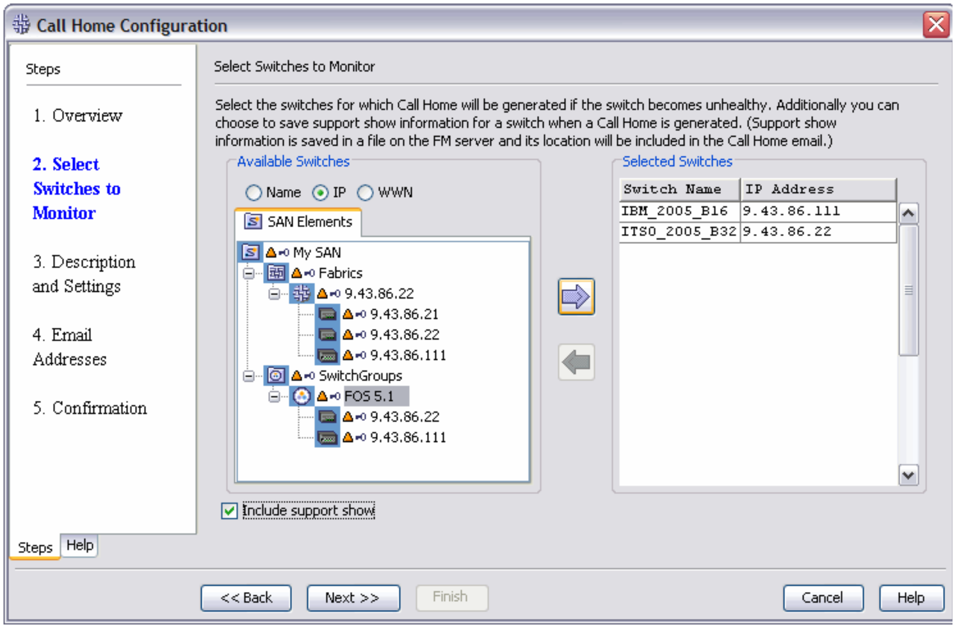


Call Home Configuration
Steps
1. Overview
2. Select Switches to Monitor
3. Description and Settings
4. Email Addresses
5. Confirmation
Steps
Help
Select Switches to Monitor
Available Switches
○ Name ● IP ○ WWN
SAN Elements
My SAN
Fabrics
9.43.86.22
9.43.86.21
9.43.86.22
9.43.86.111
SwitchGroups
FOS 5.1
9.43.86.22
9.43.86.111
Selected Switches
Switch Name
IP Address
☐ Include support show
<< Back
Next >>
Finish
Cancel
Help

Select the switches for which Call Home will be generated if the switch becomes unhealthy. Additionally you can choose to save support show information for a switch when a Call Home is generated. (Support show information is saved in a file on the FM server and its location will be included in the Call Home email.)

Figure 1-192   Select switches to monitor

We now select the appropriate switches and click the right-hand arrow, see Figure 1-193. This adds them into the selected switches box. We can also check the include support show box. This also transmits a copy of the output from the CLI command **`supportShow`**.


Call Home Configuration
Steps
1. Overview
2. Select Switches to Monitor
3. Description and Settings
4. Email Addresses
5. Confirmation
Steps
Help
Select Switches to Monitor

Select the switches for which Call Home will be generated if the switch becomes unhealthy. Additionally you can choose to save support show information for a switch when a Call Home is generated. (Support show information is saved in a file on the FM server and its location will be included in the Call Home email.)

Available Switches
○ Name ● IP ○ WWN
SAN Elements
My SAN
Fabrics
9.43.86.22
9.43.86.21
9.43.86.22
9.43.86.111
SwitchGroups
FOS 5.1
9.43.86.22
9.43.86.111
Selected Switches

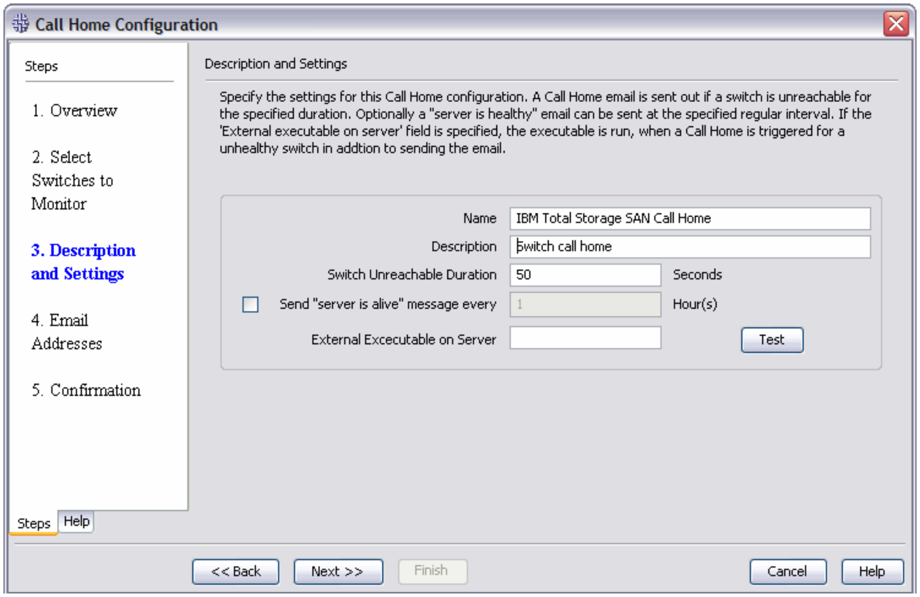
Switch Name	IP Address
IBM_2005_B16	9.43.86.111
ITSO_2005_B32	9.43.86.22

☑ Include support show

<< Back
Next >>
Finish
Cancel
Help

Figure 1-193 adding switches for call home

The next window (Figure 1-194) in the Wizard requires a name and description for this particular call-home profile. Optionally, we can enable server monitoring via an executable program stored on the FM server which can acknowledge whether a particular server is alive or not.


Call Home Configuration
Steps
1. Overview
2. Select Switches to Monitor
3. Description and Settings
4. Email Addresses
5. Confirmation
Steps
Help
Test
<< Back
Next >>
Finish
Cancel
Help

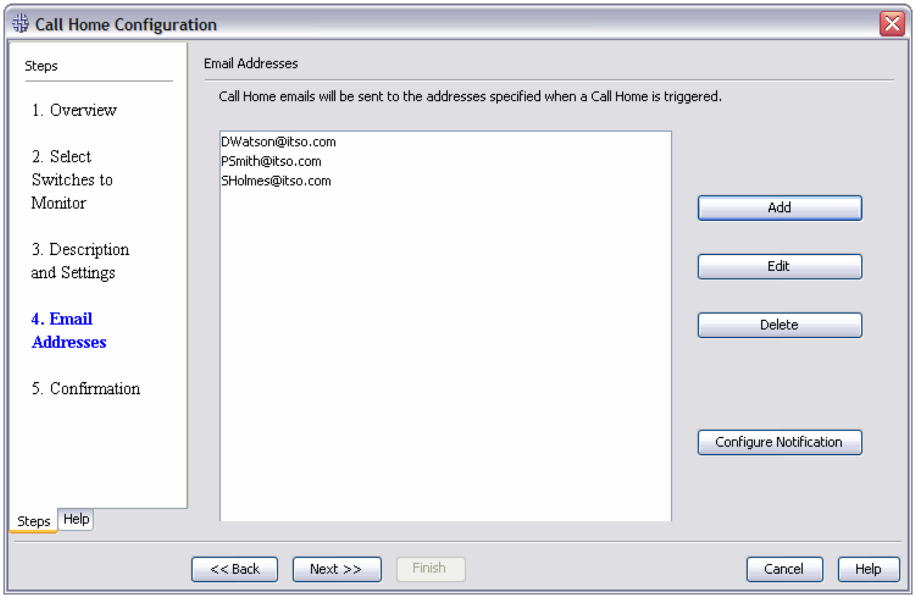
Description and Settings

Specify the settings for this Call Home configuration. A Call Home email is sent out if a switch is unreachable for the specified duration. Optionally a "server is healthy" email can be sent at the specified regular interval. If the 'External executable on server' field is specified, the executable is run, when a Call Home is triggered for a unhealthy switch in addtion to sending the email.

Name: IBM Total Storage SAN Call Home
Description: Switch call home
Switch Unreachable Duration: 50 Seconds
☐ Send "server is alive" message every: 1 Hour(s)
External Excecutable on Server:

Figure 1-194 Call Home Configuration description

Here, in Figure 1-195, we add the appropriate e-mail addresses.


Call Home Configuration
Steps
1. Overview
2. Select Switches to Monitor
3. Description and Settings
4. Email Addresses
5. Confirmation
Steps
Help
Add
Edit
Delete
Configure Notification
<< Back
Next >>
Finish
Cancel
Help

Email Addresses

Call Home emails will be sent to the addresses specified when a Call Home is triggered.

DWatson@itso.com
PSmith@itso.com
SHolmes@itso.com

Figure 1-195 Adding e-mail recipients

After selecting **Next** and reviewing the final summary panel, the call home setup is now complete. If, however, you have not already configured an e-mail server, the appropriate window is displayed to do so now. From the Notification Configuration panel (Figure 1-196), you can opt to send a test e-mail to confirm that the service is functioning correctly. As well as this, you can test the call home setup by disabling an unused port. This sets a marginal status on the disabled port, and after the specified monitoring interval, trigger an e-mail to be sent.

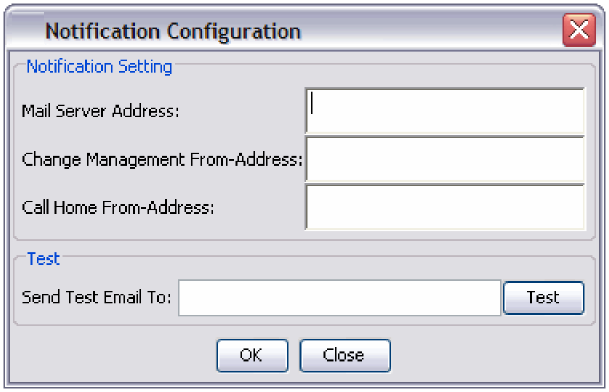

Notification Configuration
Notification Setting
Mail Server Address:
Change Management From-Address:
Call Home From-Address:
Test
Send Test Email To:
Test
OK
Close

Figure 1-196 Call Home Notification Configuration

After configuring Call Home, the e-mail recipients receive an e-mail containing the following text:

```
You are going to be receiving email if any of the switches listed in the
'IBM Total Storage SAN Call Home' configuration becomes unhealthy.
```

Whenever events are triggered, these are e-mailed to the recipients in XML format as shown in Example 1-22. Notice that the e-mail also contains an XML attachment detailing the trigger. The XML file has not been included in our example for clarity.

Example 1-22 E-mail trigger events

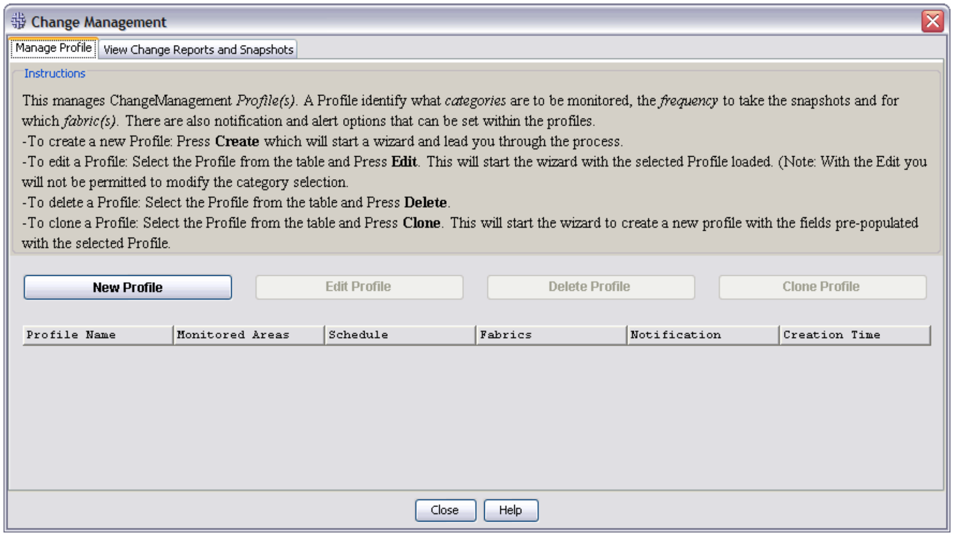
```
<?xml version="1.0" encoding="UTF-8"?>
<CallHomeAlert type="statusUnhealthy" serverName="IBM-94B6002CA8B"
serverIP="66.243.40.188" time="Aug 26, 2006 6:21:39 AM BST"
epochTime="1156569699162" >
<Briefing>Call home is triggered on switch IBM_2005_B16
(wwn=10:00:00:05:1e:02:4e:fb ip=9.43.86.111 fcIp=0.0.0.0) of group IBM Total
Storage SAN Call Home because switch status turns to Marginal</Briefing>
<TriggerEvent>
<StatusEvent status="Marginal"> <Reason> Switch Status is MARGINAL.
Contributors:
* Marginal Port: 1(4) (MARGINAL).</Reason>
```

```
</StatusEvent>
</TriggerEvent>
<Source>
<Switch name="IBM_2005_B16" wwn="10:00:00:05:1e:02:4e:fb"
ethernetIP="9.43.86.111" ethernetIPMask="255.255.255.0" fcIP="0.0.0.0"
fcIPMask="0.0.0.0" firmware="v5.1.0b" switchType="34" domainID="3"
factorySerialNumber="RD060024766" supplierSerialNumber="100856D"/>
</Source>
</CallHomeAlert>
```

New Change Management Wizard

Fabric Manager can now be configured to monitor and maintain configuration and status knowledge of switches and directors within your SANs. The Change Management functionality allows you to save “snapshot” images from switches which can be compared, to identify any changes in, for example: firmware levels, ISLs, Security Policies, and Fabric Membership. When any of these monitored items change, then an e-mail notification is sent to a pre-defined list of users.

The Change Management Wizard is accessed via the pull-down menu, **Tools** → **Change Management** → **Manage Profiles**. See Figure 1-197.

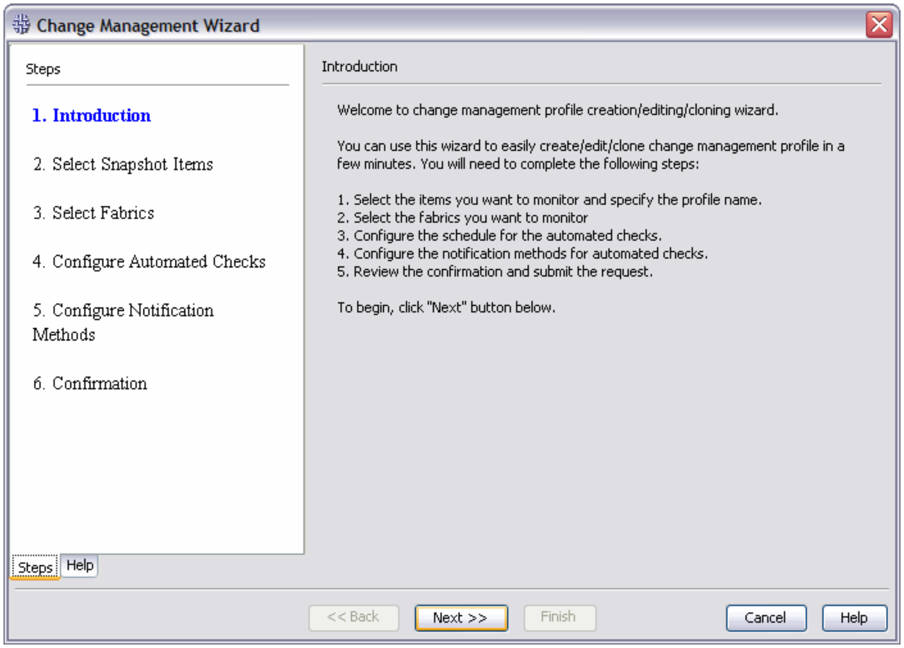

Change Management
Manage Profile
View Change Reports and Snapshots
Instructions

This manages ChangeManagement *Profile(s)*. A Profile identify what *categories* are to be monitored, the *frequency* to take the snapshots and for which *fabric(s)*. There are also notification and alert options that can be set within the profiles.
-To create a new Profile: Press **Create** which will start a wizard and lead you through the process.
-To edit a Profile: Select the Profile from the table and Press **Edit**. This will start the wizard with the selected Profile loaded. (Note: With the Edit you will not be permitted to modify the category selection.
-To delete a Profile: Select the Profile from the table and Press **Delete**.
-To clone a Profile: Select the Profile from the table and Press **Clone**. This will start the wizard to create a new profile with the fields pre-populated with the selected Profile.

New Profile
Edit Profile
Delete Profile
Clone Profile
Profile Name
Monitored Areas
Schedule
Fabrics
Notification
Creation Time
Close
Help

Figure 1-197 Initial window from Manage Profiles menu selection

As we select a new profile from here, we launch into the wizard itself, seen in Figure 1-198.


Change Management Wizard
Steps
1. Introduction
2. Select Snapshot Items
3. Select Fabrics
4. Configure Automated Checks
5. Configure Notification Methods
6. Confirmation
Steps
Help
<< Back
Next >>
Finish
Cancel
Help

Introduction

Welcome to change management profile creation/editing/cloning wizard.

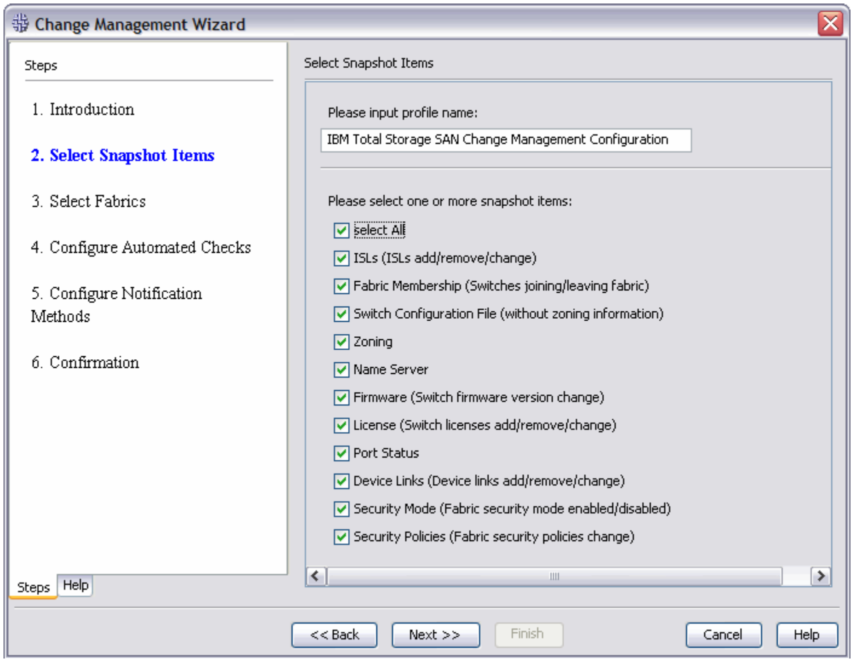
You can use this wizard to easily create/edit/clone change management profile in a few minutes. You will need to complete the following steps:

1. Select the items you want to monitor and specify the profile name.
2. Select the fabrics you want to monitor
3. Configure the schedule for the automated checks.
4. Configure the notification methods for automated checks.
5. Review the confirmation and submit the request.

To begin, click "Next" button below.

Figure 1-198 Change Management Wizard Introduction

After the introduction window, we are presented with a new window listing all the events which can be monitored, shown in Figure 1-199. The first option is **Select All**. A profile name is also required.


Change Management Wizard
Steps
1. Introduction
2. Select Snapshot Items
3. Select Fabrics
4. Configure Automated Checks
5. Configure Notification Methods
6. Confirmation
Steps
Help
Select Snapshot Items
<< Back
Next >>
Finish
Cancel
Help

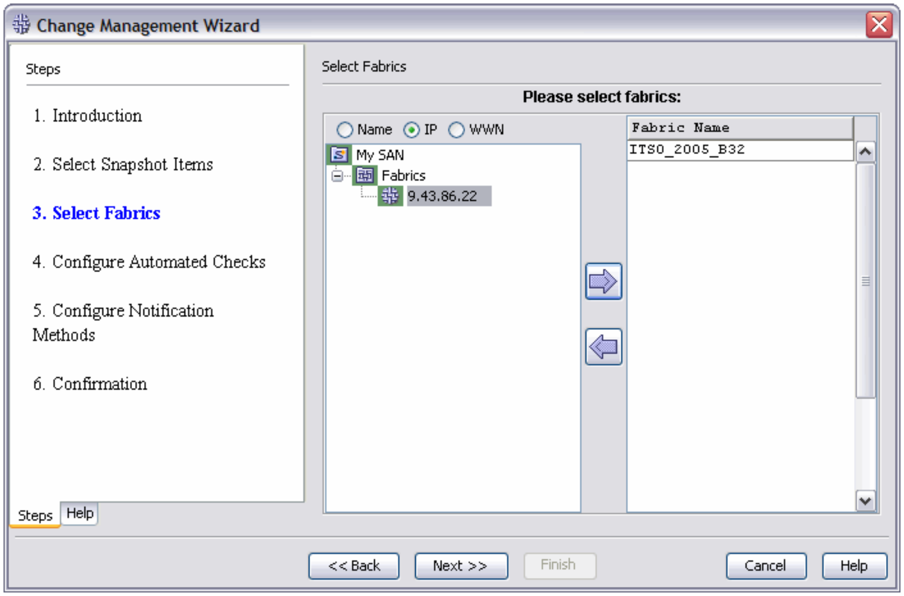
Please input profile name:
IBM Total Storage SAN Change Management Configuration

Please select one or more snapshot items:

☑ Select All
☑ ISLs (ISLs add/remove/change)
☑ Fabric Membership (Switches joining/leaving fabric)
☑ Switch Configuration File (without zoning information)
☑ Zoning
☑ Name Server
☑ Firmware (Switch firmware version change)
☑ License (Switch licenses add/remove/change)
☑ Port Status
☑ Device Links (Device links add/remove/change)
☑ Security Mode (Fabric security mode enabled/disabled)
☑ Security Policies (Fabric security policies change)

Figure 1-199 A fully populated Change Management Wizard window

When we have selected the information required to be monitored, we move on to selecting which switches require monitoring, as seen in Figure 1-200.


Change Management Wizard
Steps
1. Introduction
2. Select Snapshot Items
3. Select Fabrics
4. Configure Automated Checks
5. Configure Notification Methods
6. Confirmation
Steps
Help
<< Back
Next >>
Finish
Cancel
Help

Select Fabrics

Please select fabrics:

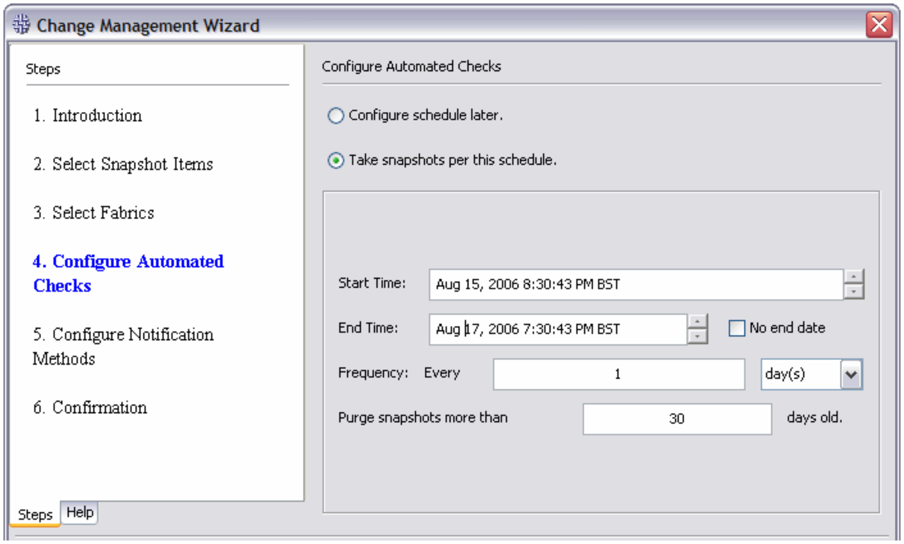
○ Name ● IP ○ WWN

- My SAN
  - Fabrics
    - 9.43.86.22

Fabric Name
ITSO_2005_B32

Figure 1-200 Selecting the switches which we want to monitor

Now that we have selected our switches, we can specify how often the snapshots of data should be taken. See Figure 1-201.


Change Management Wizard
Steps
1. Introduction
2. Select Snapshot Items
3. Select Fabrics
4. Configure Automated Checks
5. Configure Notification Methods
6. Confirmation
Steps
Help

Configure Automated Checks

○ Configure schedule later.

● Take snapshots per this schedule.

Start Time: Aug 15, 2006 8:30:43 PM BST

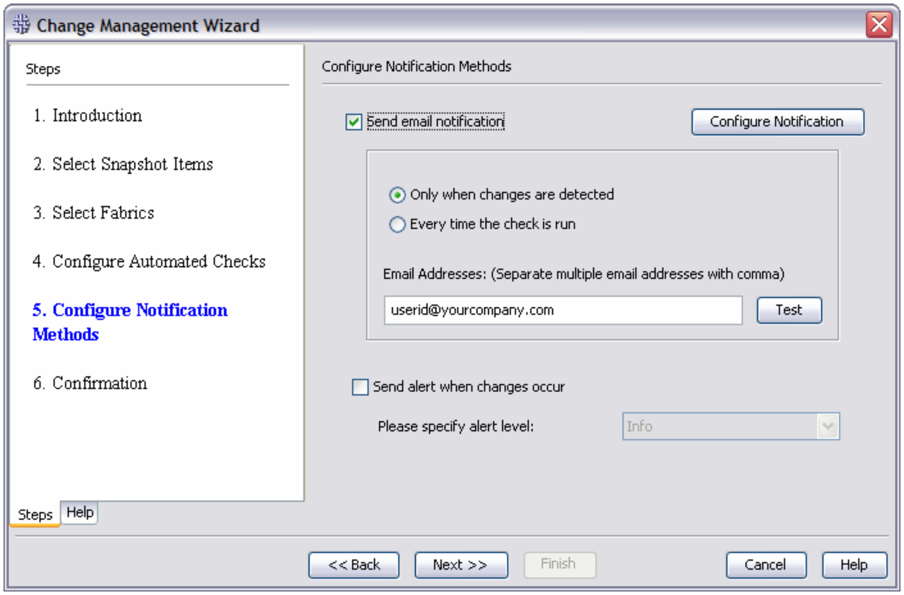
End Time: Aug 17, 2006 7:30:43 PM BST ☐ No end date

Frequency: Every 1 day(s)

Purge snapshots more than 30 days old.

Figure 1-201 How often the automated checks should run

We are now in a position to add a required receiver for the notification of a change in the monitored settings shown in Figure 1-202.



Steps

1. Introduction
2. Select Snapshot Items
3. Select Fabrics
4. Configure Automated Checks
5. **Configure Notification Methods**
6. Confirmation

Configure Notification Methods

☑ Send email notification

● Only when changes are detected
○ Every time the check is run

Email Addresses: (Separate multiple email addresses with comma)
userid@yourcompany.com

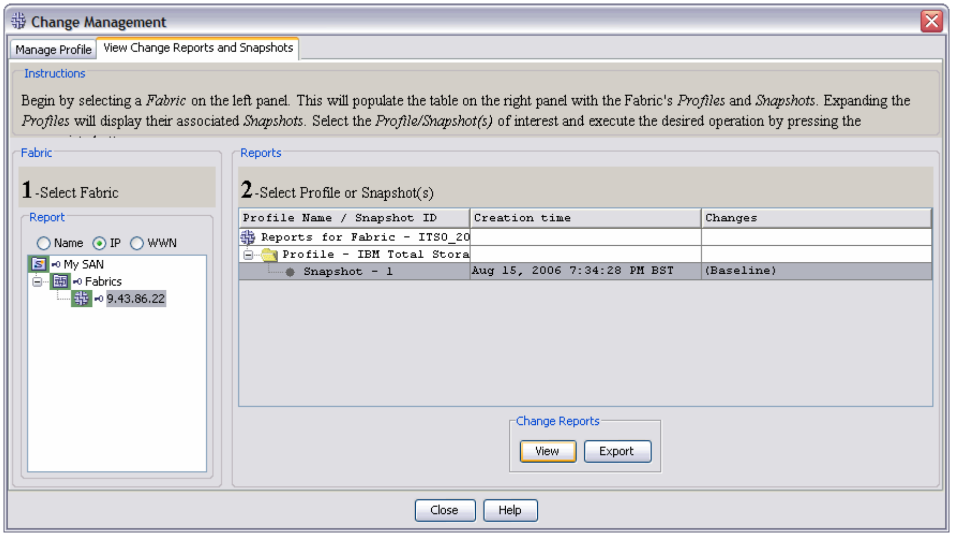
☐ Send alert when changes occur

Please specify alert level: Info

Figure 1-202 Selecting a recipient of the alert

Now that we have completed the setup, we are in a position to test this monitoring service by triggering one of the monitored events. Before completing the wizard, you have to confirm your selections, then click the **Finish** button. The system then proceeds to process the request, after which you are advised that the profile has been successfully created/edited/cloned. You then see your newly created profile in the Manage profile tab of the Change Management window.

We can also view change reports and snapshots by selecting the tab as detailed in Figure 1-203.


Change Management
Manage Profile
View Change Reports and Snapshots
Instructions
Fabric
1-Select Fabric
Report
○ Name ● IP ○ WWN
My SAN
Fabrics
9.43.86.22
Reports
2-Select Profile or Snapshot(s)
Change Reports
View
Export
Close
Help

Begin by selecting a *Fabric* on the left panel. This will populate the table on the right panel with the Fabric's *Profiles* and *Snapshots*. Expanding the *Profiles* will display their associated *Snapshots*. Select the *Profile/Snapshot(s)* of interest and execute the desired operation by pressing the

Profile Name / Snapshot ID	Creation time	Changes
Reports for Fabric - ITSO_20		
Profile - IBM Total Stora		
Snapshot - 1	Aug 15, 2006 7:34:28 PM BST	(Baseline)

Figure 1-203 Change Management Reports and Snapshots tab

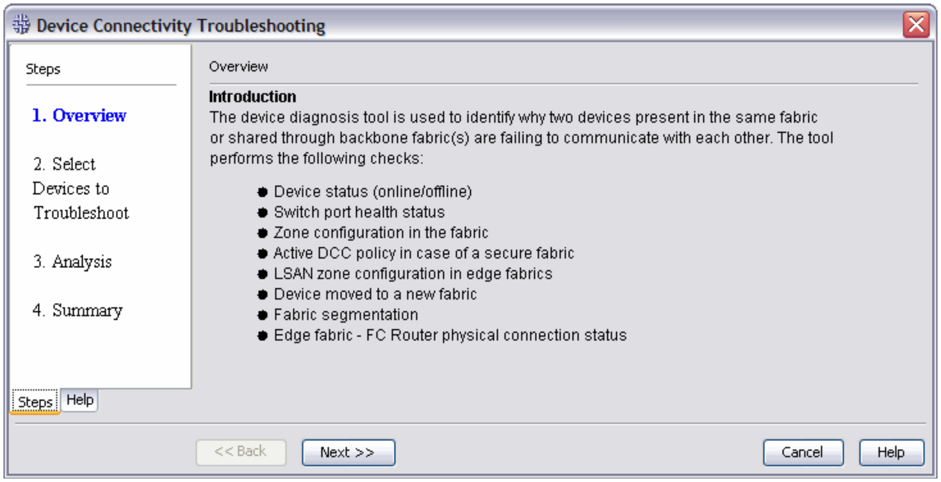
Device Connectivity Troubleshooting Wizard

This tool allows you to select two devices in the same fabric, for example, a host HBA and a storage port, and have the following checks performed upon them: device status, switch port health status, zoning configuration, and security policy check.

Further checks are also performed, and a full list of these checks is displayed in the initial wizard startup panel.

To initiate the Device Connectivity Troubleshooting Wizard, we select from the drop-down menus: **Tools** → **Device Connectivity Troubleshooting**.

An example of this is shown in Figure 1-204.


Device Connectivity Troubleshooting
Steps
1. Overview
2. Select Devices to Troubleshoot
3. Analysis
4. Summary
Steps
Help
<< Back
Next >>
Cancel
Help

Overview

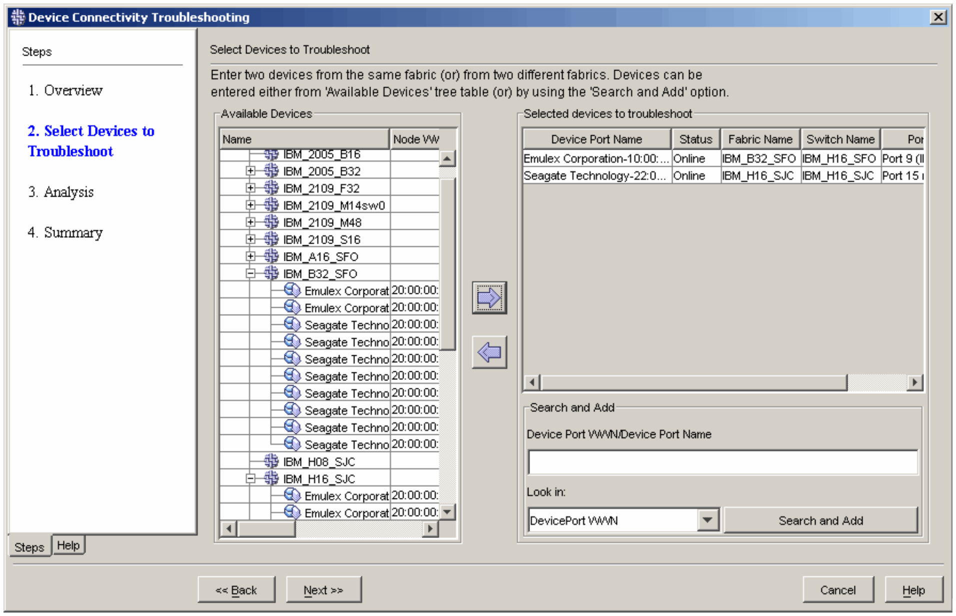
Introduction

The device diagnosis tool is used to identify why two devices present in the same fabric or shared through backbone fabric(s) are failing to communicate with each other. The tool performs the following checks:

- Device status (online/offline)
- Switch port health status
- Zone configuration in the fabric
- Active DCC policy in case of a secure fabric
- LSAN zone configuration in edge fabrics
- Device moved to a new fabric
- Fabric segmentation
- Edge fabric - FC Router physical connection status

Figure 1-204 Initial device troubleshooting wizard panel

On the following panel, Figure 1-205, we select the devices we are interested in.


Device Connectivity Troubleshooting
Steps
1. Overview
2. Select Devices to Troubleshoot
3. Analysis
4. Summary
Steps
Help
Search and Add
<< Back
Next >>
Cancel
Help

Select Devices to Troubleshoot

Enter two devices from the same fabric (or) from two different fabrics. Devices can be entered either from 'Available Devices' tree table (or) by using the 'Search and Add' option.

Available Devices

Name	Node WW
IBM_2005_B16	
IBM_2005_B32	
IBM_2109_F32	
IBM_2109_M14sw0	
IBM_2109_M48	
IBM_2109_S16	
IBM_A16_SFO	
IBM_B32_SFO	
Emulex Corporat	20:00:00:
Emulex Corporat	20:00:00:
Seagate Techno	20:00:00:
Seagate Techno	20:00:00:
Seagate Techno	20:00:00:
Seagate Techno	20:00:00:
Seagate Techno	20:00:00:
Seagate Techno	20:00:00:
Seagate Techno	20:00:00:
Seagate Techno	20:00:00:
IBM_H08_SJC	
IBM_H16_SJC	
Emulex Corporat	20:00:00:
Emulex Corporat	20:00:00:

Selected devices to troubleshoot

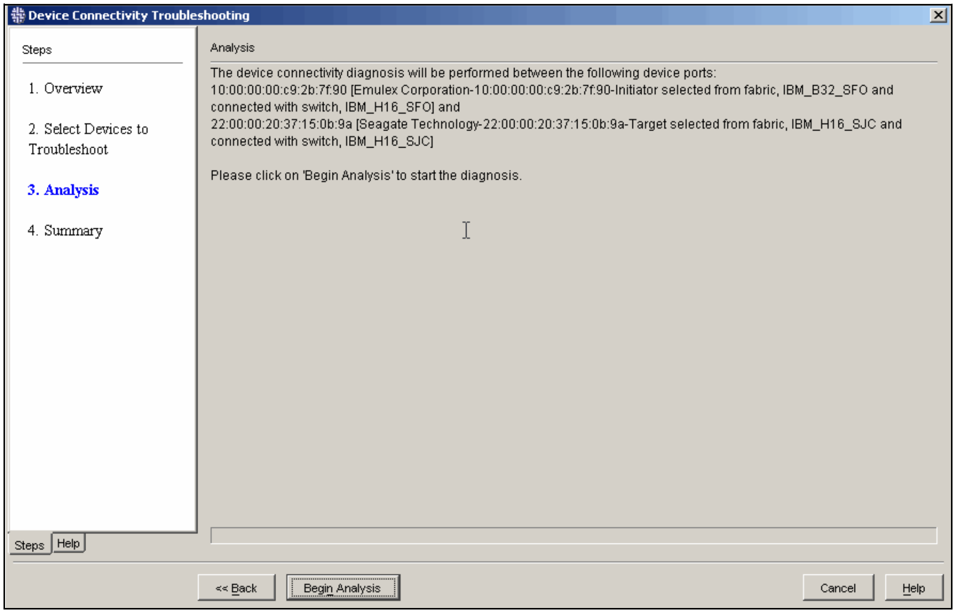
Device Port Name	Status	Fabric Name	Switch Name	Por
Emulex Corporation-10:00:...	Online	IBM_B32_SFO	IBM_H16_SFO	Port 9 (I
Seagate Technology-22:0...	Online	IBM_H16_SJC	IBM_H16_SJC	Port 15

Device Port WWN/Device Port Name:

Look in: DevicePort WWN

Figure 1-205 Selecting end-ports

Now we can initiate the analysis phase of the checking as shown in Figure 1-206.

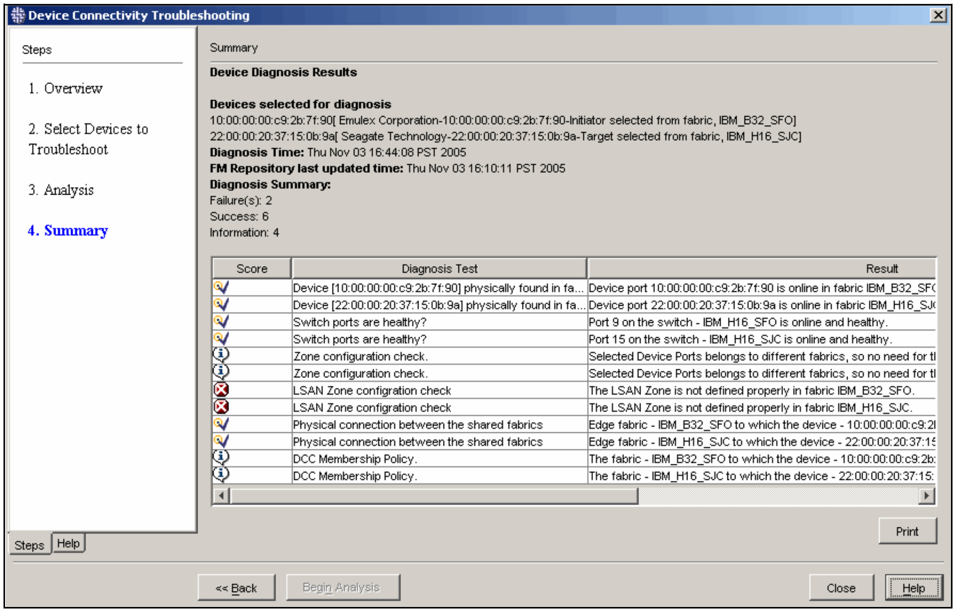

Device Connectivity Troubleshooting
Steps
1. Overview
2. Select Devices to Troubleshoot
3. Analysis
4. Summary
Steps
Help
Analysis
<< Back
Begin Analysis
Cancel
Help

The device connectivity diagnosis will be performed between the following device ports:
10:00:00:00:c9:2b:7f:90 [Emulex Corporation-10:00:00:00:c9:2b:7f:90-Initiator selected from fabric, IBM_B32_SFO and connected with switch, IBM_H16_SFO] and
22:00:00:20:37:15:0b:9a [Seagate Technology-22:00:00:20:37:15:0b:9a-Target selected from fabric, IBM_H16_SJC and connected with switch, IBM_H16_SJC]

Please click on 'Begin Analysis' to start the diagnosis.

Figure 1-206 Starting the analysis

After a few moments, the analysis is complete and a final summary window displays our results. This window can be seen in Figure 1-207.



Device Diagnosis Results

Devices selected for diagnosis
10:00:00:00:c9:2b:7f:90[Emulex Corporation-10:00:00:00:c9:2b:7f:90-Initiator selected from fabric, IBM_B32_SFO]
22:00:00:20:37:15:0b:9a[Seagate Technology-22:00:00:20:37:15:0b:9a-Target selected from fabric, IBM_H16_SJC]
Diagnosis Time: Thu Nov 03 16:44:08 PST 2005
FM Repository last updated time: Thu Nov 03 16:10:11 PST 2005
Diagnosis Summary:
Failure(s): 2
Success: 6
Information: 4

Score	Diagnosis Test	Result
✓	Device [10:00:00:00:c9:2b:7f:90] physically found in fa...	Device port 10:00:00:00:c9:2b:7f:90 is online in fabric IBM_B32_SF
✓	Device [22:00:00:20:37:15:0b:9a] physically found in fa...	Device port 22:00:00:20:37:15:0b:9a is online in fabric IBM_H16_SJ
✓	Switch ports are healthy?	Port 9 on the switch - IBM_H16_SFO is online and healthy.
✓	Switch ports are healthy?	Port 15 on the switch - IBM_H16_SJC is online and healthy.
ⓘ	Zone configuration check.	Selected Device Ports belongs to different fabrics, so no need for t
ⓘ	Zone configuration check.	Selected Device Ports belongs to different fabrics, so no need for t
⊗	LSAN Zone configration check	The LSAN Zone is not defined properly in fabric IBM_B32_SFO.
⊗	LSAN Zone configration check	The LSAN Zone is not defined properly in fabric IBM_H16_SJC.
✓	Physical connection between the shared fabrics	Edge fabric - IBM_B32_SFO to which the device - 10:00:00:00:c9:2
✓	Physical connection between the shared fabrics	Edge fabric - IBM_H16_SJC to which the device - 22:00:00:20:37:1
ⓘ	DCC Membership Policy.	The fabric - IBM_B32_SFO to which the device - 10:00:00:00:c9:2b:
ⓘ	DCC Membership Policy.	The fabric - IBM_H16_SJC to which the device - 22:00:00:20:37:15:

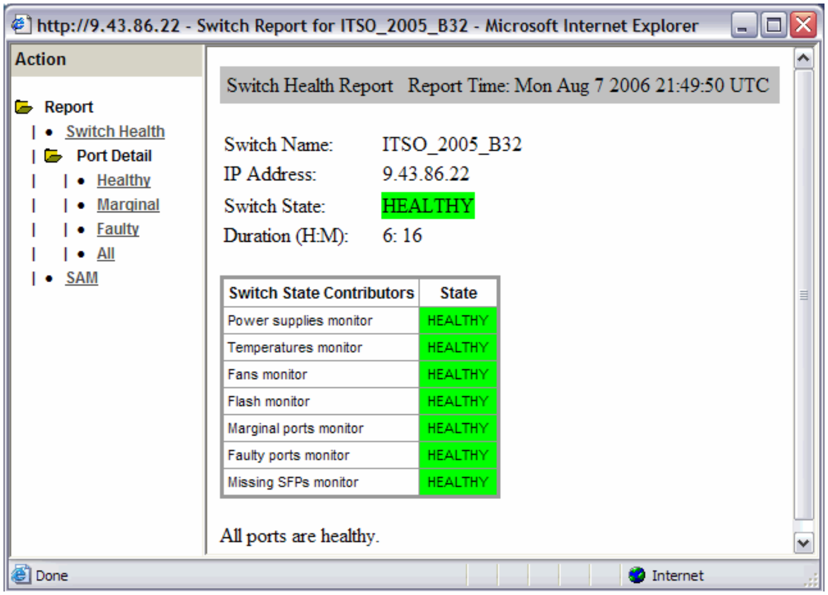
Figure 1-207 Completed Analysis

From here we can see the results of the various tests performed. Notice that we triggered some failures, and here we ran a check for LSAN zone information. As the two ports chosen were not routed across separate fabrics, they would not be part of an LSAN — therefore these failures in this configuration can be ignored.

Fabric Manager Reports

Two types of report are available within Fabric Manager, these are the Switch Health and SAN Health reports. Both of these reports are found in the Reports drop-down menu.

The Switch Health report is the same as that viewed via the Web Tools Status button and is displayed for your reference in Figure 1-208.


http://9.43.86.22 - Switch Report for ITSO_2005_B32 - Microsoft Internet Explorer
Action
Report
Switch Health
Port Detail
Healthy
Marginal
Faulty
All
SAM
Done
Internet

Switch Health Report Report Time: Mon Aug 7 2006 21:49:50 UTC

Switch Name: ITSO_2005_B32
IP Address: 9.43.86.22
Switch State: HEALTHY
Duration (H:M): 6: 16

Switch State Contributors	State
Power supplies monitor	HEALTHY
Temperatures monitor	HEALTHY
Fans monitor	HEALTHY
Flash monitor	HEALTHY
Marginal ports monitor	HEALTHY
Faulty ports monitor	HEALTHY
Missing SFPs monitor	HEALTHY

All ports are healthy.

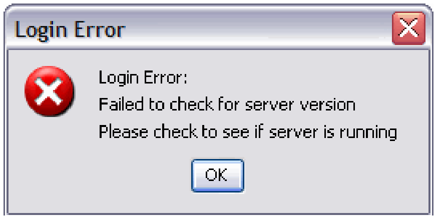
Figure 1-208 Switch Health Report via Fabric Manager

In order to select the SAN Health reports option, you must have previously installed the SAN Health tool. When you select this option, the SAN Health tool launches. Refer to 1.10.1, “SAN Health” on page 329 for further details.

We have covered only a selection of the features, new and current, of Fabric Manager. For full details of all the features, refer to the appropriate version of the *Fabric Manager Administrator’s Guide,* 53-1000042, which is downloadable from the Web site: `http://www.brocade.com`

1.9.6 Troubleshooting Fabric Manager

If there is a problem with the Fabric Manager server, you might get a Login error that advises you to check whether the server is running. An example of this is shown in Figure 1-209.

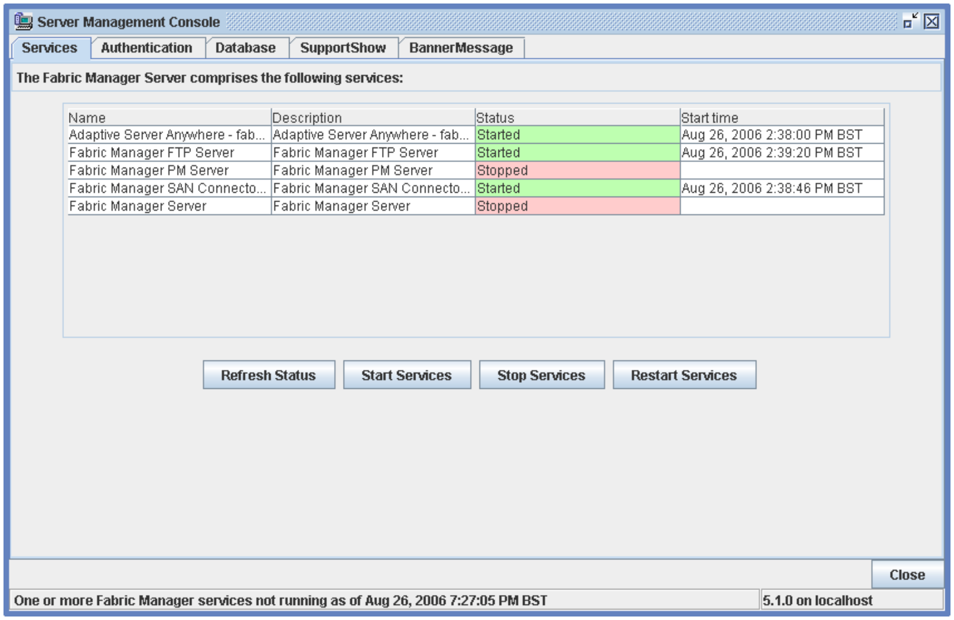

Login Error
OK

Login Error:
Failed to check for server version
Please check to see if server is running

Figure 1-209 Fabric Manager login error

To check the status of the Fabric Manager services, we log in to the Fabric Manager Server Management Console. If our Fabric Manager server is installed on a Windows server we access this by clicking the **Start** button, then selecting **All Programs** → **Fabric Manager** → **Server Management Console**.

As the console starts, the current status of the Fabric manager services is assessed. In our example we can see that the Fabric Manager PM server and the Fabric Manager server itself are stopped, as shown in Figure 1-210.


Server Management Console
Services
Authentication
Database
SupportShow
BannerMessage
Refresh Status
Start Services
Stop Services
Restart Services
Close

The Fabric Manager Server comprises the following services:

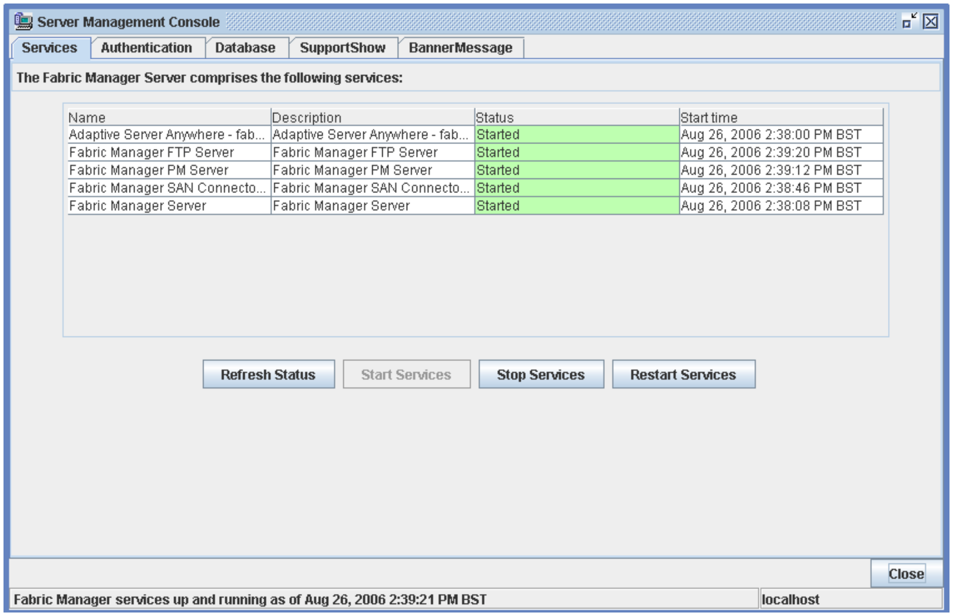
Name	Description	Status	Start time
Adaptive Server Anywhere - fab...	Adaptive Server Anywhere - fab...	Started	Aug 26, 2006 2:38:00 PM BST
Fabric Manager FTP Server	Fabric Manager FTP Server	Started	Aug 26, 2006 2:39:20 PM BST
Fabric Manager PM Server	Fabric Manager PM Server	Stopped	
Fabric Manager SAN Connecto...	Fabric Manager SAN Connecto...	Started	Aug 26, 2006 2:38:46 PM BST
Fabric Manager Server	Fabric Manager Server	Stopped	

One or more Fabric Manager services not running as of Aug 26, 2006 7:27:05 PM BST

5.1.0 on localhost

Figure 1-210 Fabric Manager Server Management Console with stopped services

In order to resolve this problem, we restart the services by clicking the **Restart Services** button. When the restart completes, we see all the services in a started state, as shown in Figure 1-211.



The Fabric Manager Server comprises the following services:

Name	Description	Status	Start time
Adaptive Server Anywhere - fab...	Adaptive Server Anywhere - fab...	Started	Aug 26, 2006 2:38:00 PM BST
Fabric Manager FTP Server	Fabric Manager FTP Server	Started	Aug 26, 2006 2:39:20 PM BST
Fabric Manager PM Server	Fabric Manager PM Server	Started	Aug 26, 2006 2:39:12 PM BST
Fabric Manager SAN Connecto...	Fabric Manager SAN Connecto...	Started	Aug 26, 2006 2:38:46 PM BST
Fabric Manager Server	Fabric Manager Server	Started	Aug 26, 2006 2:38:08 PM BST

Fabric Manager services up and running as of Aug 26, 2006 2:39:21 PM BST

Figure 1-211 Fabric Manager Server Management Console with started services

We can now re-attempt our log in to the Fabric Manager application. During our testing, we found that in some cases although the Server Management Console indicated that the services were all started, we were still unable to log in to Fabric Manager. If you have a similar problem, it might be necessary to check that the services are running at the operating system level.

On a Windows server, this can be done by right-clicking the **My Computer** icon and selecting **Manage** from the drop down menu. Select **Services & Applications** from the Computer Management panel, and then **Services**. Look for the Fabric Manager services, as shown in Figure 1-211, and stop or restart them as appropriate. When they are all running, you should then be able to log into Fabric Manager from your client.

You can also use the Server Management Console to check the status of your in-built FTP server as well as change the authentication method used for logging in to Fabric Manager.

1.9.7 Upgrading the switch

From time to time, new versions of firmware are released. In the following example, we have documented the steps to upgrade a switch to v5.1.0 FOS code. This can be performed using Telnet or by using the WebTools interface. We perform both methods.

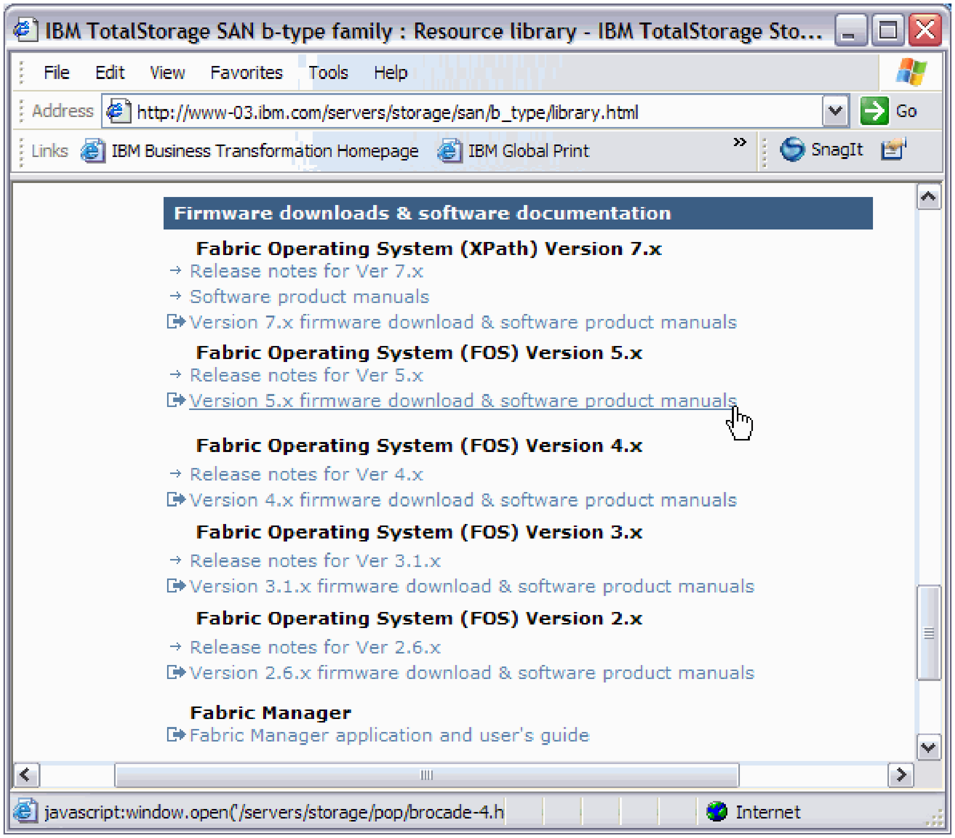
The latest microcode levels can be obtained for the various switches from the IBM support Web site. The following link provides documentation downloads as well as the links to the firmware downloads:

`http://www-1.ibm.com/servers/storage/san/b_type/library.html#downloads`

> **Note:** As new firmware levels are introduced regularly, the process we document here applies to subsequent firmware releases. At the time of writing, we chose the most current levels.

In this example we went to the IBM support Web site and chose the following link for the Version 5.x firmware download, as shown in Figure 1-212:

`http://www-1.ibm.com/servers/storage/san/b_type/library.html#downloads`


IBM TotalStorage SAN b-type family : Resource library - IBM TotalStorage Sto...
File
Edit
View
Favorites
Tools
Help
Address
http://www-03.ibm.com/servers/storage/san/b_type/library.html
Go
Links
IBM Business Transformation Homepage
IBM Global Print
SnagIt
Internet

Firmware downloads & software documentation

Fabric Operating System (XPath) Version 7.x
- Release notes for Ver 7.x
- Software product manuals
- Version 7.x firmware download & software product manuals

Fabric Operating System (FOS) Version 5.x
- Release notes for Ver 5.x
- Version 5.x firmware download & software product manuals

Fabric Operating System (FOS) Version 4.x
- Release notes for Ver 4.x
- Version 4.x firmware download & software product manuals

Fabric Operating System (FOS) Version 3.x
- Release notes for Ver 3.1.x
- Version 3.1.x firmware download & software product manuals

Fabric Operating System (FOS) Version 2.x
- Release notes for Ver 2.6.x
- Version 2.6.x firmware download & software product manuals

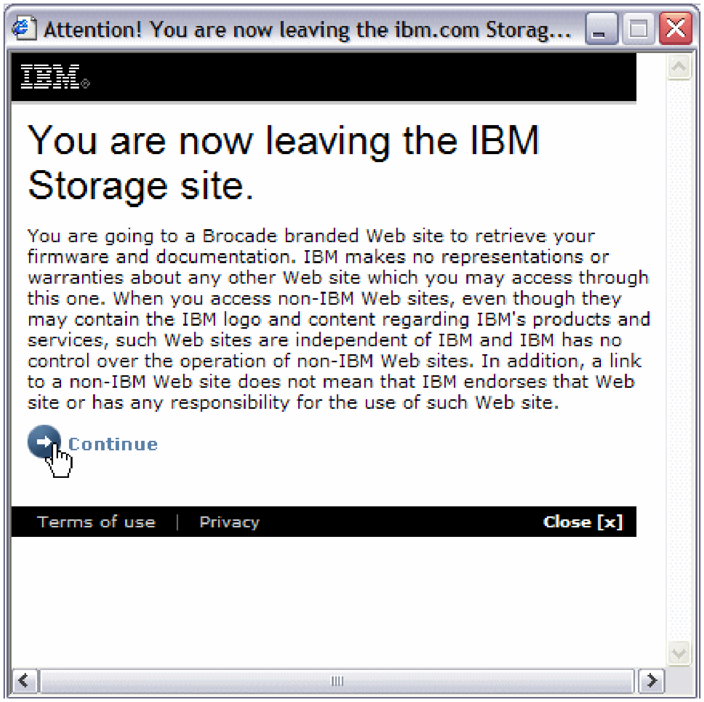
Fabric Manager
- Fabric Manager application and user's guide

javascript:window.open('/servers/storage/pop/brocade-4.h

Figure 1-212 IBM product support Web page

We can arrive at the above Web link in a number of ways. When viewing the product details for any switch, just look for the tab or arrow entitled **Downloads**. By clicking **Downloads**, it brings us to all the available downloads for all models.

By clicking the Version 5.x firmware download link, it redirects us to the Brocade download site, which allows us to download firmware and documentation for all of the IBM TotalStorage SAN Switch products. A pop-up window appears warning us of the redirection off the IBM hosted Web site shown in Figure 1-213.



You are now leaving the IBM Storage site.

You are going to a Brocade branded Web site to retrieve your firmware and documentation. IBM makes no representations or warranties about any other Web site which you may access through this one. When you access non-IBM Web sites, even though they may contain the IBM logo and content regarding IBM's products and services, such Web sites are independent of IBM and IBM has no control over the operation of non-IBM Web sites. In addition, a link to a non-IBM Web site does not mean that IBM endorses that Web site or has any responsibility for the use of such Web site.

Figure 1-213 Redirect to Brocade confirmation

We click **Continue** and arrive at the Brocade downloads Web site shown in Figure 1-214, where it shows all available levels. From here, we select the **V5.1.x Firmware** and are directed to all available downloads for V5.1.x.

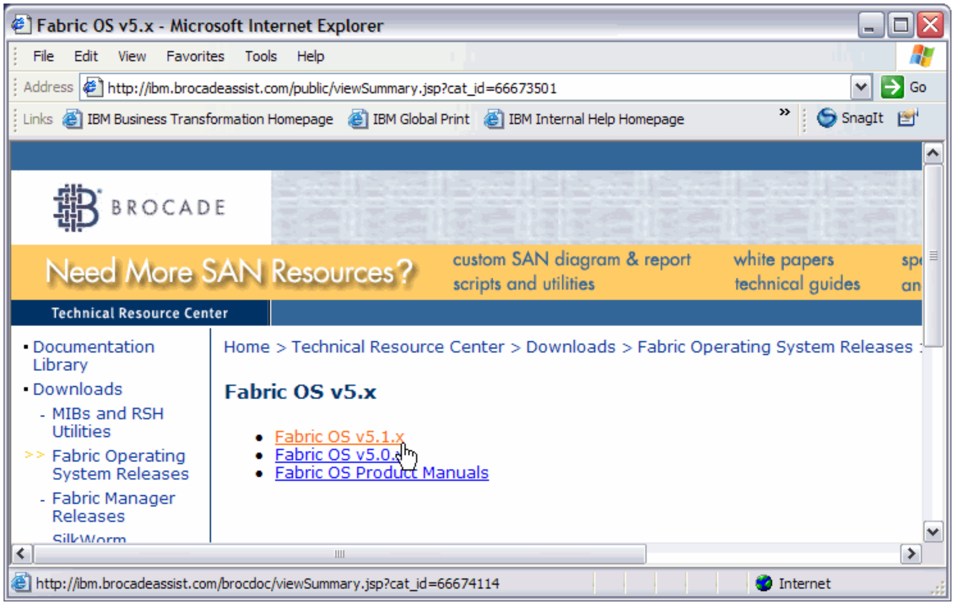

Fabric OS v5.x - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://ibm.brocadeassist.com/public/viewSummary.jsp?cat_id=66673501
Go
Links IBM Business Transformation Homepage IBM Global Print IBM Internal Help Homepage
SnagIt
BROCADE
Need More SAN Resources?
custom SAN diagram & report
scripts and utilities
white papers
technical guides
Technical Resource Center
Documentation Library
Downloads
MIBs and RSH Utilities
Fabric Operating System Releases
Fabric Manager Releases
SilkWorm
Home > Technical Resource Center > Downloads > Fabric Operating System Releases
Fabric OS v5.x
Fabric OS v5.1.x
Fabric OS v5.0.x
Fabric OS Product Manuals
http://ibm.brocadeassist.com/brocdoc/viewSummary.jsp?cat_id=66674114
Internet

Figure 1-214 Brocade Web Firmware levels download list

> **Tip:** When selecting the latest level to download, always ensure that it is compatible with other hardware in the SAN.

When we have selected a firmware level to download, we are prompted to provide our company name and address as information. When the code is downloaded, then we are able to unzip the files to prepare for the install. In our example, we downloaded the Windows version and stored the files on a Windows server.

The firmware can be downloaded to the switch in one of the following ways:

- Telnet session
- WebTools administration functions
- Fabric Manager

If you are running Fabric OS 4.1 or later the firmware update process provides hot code activation. The firmware update initially takes place to the secondary partition within the switches CP. The secondary partition is then promoted to primary, while the firmware is downloaded to the original primary partition, because such a reboot is not required in order to activate the new firmware release. The ASICs remain running throughout the operation and all connected devices should remain available.

In the sections that follow we detail a standard firmware update via telnet to a SAN16B switch. We then detail the upgrade process for a SAN256B switch, as well as a staged upgrade that can be used to allow an upgrade to be tested prior to committing. We also detail the firmware upgrade process to the SAN256B via Web tools.

Important: Before downloading firmware to your switches be sure to read the release notes to check for any issues that might be related to that version.

After you have started the firmware update process, you must not enter disruptive commands or disconnect the switch from the power, because this can render the switch inoperable. The download and commit process takes approximately 17 minutes, though is switch dependant. If a problem occurs, you have to wait for the time-out (30 minutes for network issues).

Upgrading the firmware with Telnet

Before we begin the upgrade, we recommend setting the timeout value to 0, because the upgrade could take some time and the telnet session could timeout. In our example we show how to upgrade a SAN256B (M48) switch following best practice techniques.

Example 1-23 Setting the timeout value to zero

```
IBM_2109_M48:admin> timeout 0
IDLE Timeout Changed to 0 minutes
The modified IDLE Timeout will be in effect after NEXT login
IBM_2109_M48:admin>
```

After setting the value to 0, remember to logout and login again as the message indicates. In Example 1-24 we save the configuration to the host by issuing the **`configupload`** command and responding to the prompts:

Example 1-24 Saving the switch configuration

```
M48_cp1 login: admin
Password:
IBM_M48_SJC:admin> configupload
Protocol (scp or ftp) [ftp]:
Server Name or IP Address [host]: 10.64.209.228
User Name [user]: fm
File Name [config.txt]: M48_SJC_config.wri
Password:
Upload complete
IBM_M48_SJC:admin>
```

It is also useful to run the **`supportSave`** command to capture a snapshot of your configuration. This provides baseline information in case you have to troubleshoot or seek advanced support. Remember to run this command on both the primary and standby CP on directors.

Before downloading the latest firmware, we can confirm the current version using the **`firmwareShow`** command as in Example 1-25.

Example 1-25 Displaying the current Firmware version using firmwareShow

```
IBM_M48_SJC:admin> firmwareshow
Slot Name      Primary/Secondary Versions              Status
---------------------------------------------------------------
  1  FR4-18i   v5.1.0b                                  Enabled
               v5.1.0b

  5  CP0       v5.1.0b                                  Standby
               v5.1.0b

  6  CP1       v5.1.0b                                  Active *
               v5.1.0b

 10  FR4-18i   v5.1.0b                                  Enabled
               v5.1.0b
```

It is important to check that the HA environment on the SAN256B switch is fully functional with the two CPs active and synchronized before starting a firmware download. This is done using the **`haShow`** command as seen in Example 1-26.

Example 1-26 Checking that the HA state is synchronized using haShow

```
IBM_M48_SJC:admin> haShow
Local CP (Slot 5, CP0): Active, Warm Recovered
Remote CP (Slot 6, CP1): Standby, Healthy
HA enabled, Heartbeat Up, HA State synchronized
```

Now we are ready to perform the download. In our example we use the SAN256B so that we can see how the switch updates each CP and reboots. Notice that it is the CPs which reboot and not the switch itself; as such, the ASICs remain online throughout the operation.

We issue the **`firmwareDownload`** command and respond to the prompts with the IP address, the user name, file name and password as detailed in Example 1-27.

> **Important:** Firmware code files must be unzipped prior to downloading to the switch.

Example 1-27 Downloading the firmware to a SAN-256B using firmwaredownload

```
IBM_M48_SJC:admin> firmwareDownload
Server Name or IP Address: 10.64.209.228
FTP User Name: fm
File Name: /tempfos/v5.1.0c/release.plist
FTP Password:
The following AP blades are installed in the system.

Slot Name      Versions                         Traffic Disrupted
-----------------------------------------------------------------
  1  FR4-18i   v5.1.0b                                  GigE
 10  FR4-18i   v5.1.0b                                  GigE

This command will upgrade both CPs and all AP blade above. If
you want to upgrade a single CP only, please use -s option.

You can run firmwaredownloadstatus to get the status of this
command.

This command will cause the active CP to reset and will require
that existing telnet, secure telnet or SSH sessions be restarted.

Do you want to continue [Y]: y
Firmware is being downloaded to standby CP. This step may take up to 30
minutes.
Firmware has been downloaded successfully to Standby CP.
Standby CP is going to reboot with new firmware.
Standby CP booted successfully with new firmware.
```

At this point we are disconnected from the switch because the CP we were connected to has rebooted. We log back in and issue the **`firmwaredownloadstatus`** command to check on the current status of the upgrade. We already know that it has completed by the message, `Firmwaredownload has completed successfully`.

Example 1-28 Checking the firmware download status

```
IBM_M48_SJC:admin> firmwaredownloadstatus
[1]: Fri Aug 18 22:34:15 2006
Slot 5 (CP0, active): Firmware is being downloaded to standby CP. This step may
take up to 30 minutes.

[2]: Fri Aug 18 22:47:40 2006
Slot 5 (CP0, active): Firmware has been downloaded successfully to Standby CP.

[3]: Fri Aug 18 22:47:47 2006
Slot 5 (CP0, active): Standby CP is going to reboot with new firmware.
```

```
[4]: Fri Aug 18 22:49:07 2006
Slot 5 (CP0, active): Standby CP booted successfully with new firmware.

[5]: Fri Aug 18 22:49:19 2006
Slot 1 (FR4-18i): Firmware is being downloaded to the blade. This step may take
up to 10 minutes.

[6]: Fri Aug 18 22:49:20 2006
Slot 10 (FR4-18i): Firmware is being downloaded to the blade. This step may
take up to 10 minutes.

[7]: Fri Aug 18 22:50:15 2006
Slot 6 (CP1, active): Forced failover succeeded. New Active CP is running new
firmware

[8]: Fri Aug 18 22:50:23 2006
Slot 6 (CP1, active): Firmware is being download to standby CP. This step may
take up to 30 minutes.

[9]: Fri Aug 18 22:50:57 2006
Slot 10 (FR4-18i): Firmware has been downloaded successfully. Blade is
rebooting with the new firmware.

[10]: Fri Aug 18 22:50:58 2006
Slot 1 (FR4-18i): Firmware has been downloaded successfully. Blade is rebooting
with the new firmware.

[11]: Fri Aug 18 22:51:43 2006
Slot 10 (FR4-18i): Firmware commit has started on the blade. This may take up
to 10 minutes.

[12]: Fri Aug 18 22:51:44 2006
Slot 1 (FR4-18i): Firmware commit has started on the blade. This may take up to
10 minutes.

[13]: Fri Aug 18 22:52:25 2006
Slot 10 (FR4-18i): The commit operation has completed successfully.

[14]: Fri Aug 18 22:52:26 2006
Slot 1 (FR4-18i): The commit operation has completed successfully.

[15]: Fri Aug 18 23:04:02 2006
Slot 6 (CP1, active): Firmware has been downloaded successfully on Standby CP.

[16]: Fri Aug 18 23:04:09 2006
Slot 6 (CP1, active): Standby CP reboots.

[17]: Fri Aug 18 23:05:32 2006
Slot 6 (CP1, active): Standby CP booted successfully with new firmware.
```

```
[18]: Fri Aug 18 23:05:36 2006
Slot 6 (CP1, active): Firmware commit operation has started on both active and
standby CPs.

[19]: Fri Aug 18 23:10:15 2006
Slot 6 (CP1, active): Firmware commit operation has completed successfully on
both CPs.

[20]: Fri Aug 18 23:10:15 2006
Slot 6 (CP1, active): Firmwaredownload command has completed successfully. Use
firmwareshow to verify the firmware versions.
```

Now we issue the **`firmwareshow`** command to confirm that both CPs have the same firmware levels as seen in Example 1-29.

Example 1-29 Confirming the firmware status with firmwareShow

```
IBM_M48_SJC:admin> firmwareShow
Slot Name      Primary/Secondary Versions              Status
---------------------------------------------------------------
  1  FR4-18i   v5.1.0c                                  Enabled
               v5.1.0c

  5  CP0       v5.1.0c                                  Standby
               v5.1.0c

  6  CP1       v5.1.0c                                  Active *
               v5.1.0c

 10  FR4-18i   v5.1.0c                                  Enabled
               v5.1.0c
```

Notice that both of the FR4-18i routing blades were also upgraded as part of this exercise.

Finally, the **`version`** command seen in Example 1-30 shows us the system-wide version of code and at what time it was flashed.

Example 1-30 Version command

```
IBM_M48_SJC:admin> version
Kernel:     2.4.19
Fabric OS:  v5.1.0c
Made on:    Thu Jun 29 22:30:08 2006
Flash:      Fri Aug 18 22:43:38 2006
BootProm:   4.5.3
```

This completes the telnet method of firmware download and upgrade process. For more detailed information on the commands, refer to the *Brocade Fabric OS Command Reference Manual for FOS 5.1.0*, 53-1000044-02.

For completeness we also show the output from running the **`firmwaredownload`** command on a SAN16B switch in Example 1-31. Notice that although we only detail the output from the firmware download command itself, it is still appropriate to run through all the preceding steps as discussed in the SAN256B example.

Example 1-31 Running the firmwaredownload command on a SAN16B

```
IBM_2005_B16:admin> firmwaredownload
You can run firmwareDownloadStatus to get the status
of this command.

This command will cause the switch to reset and will
require that existing telnet, secure telnet or SSH
sessions be restarted.

Do you want to continue [Y]:
Server Name or IP Address: 9.43.86.49
User Name: root
File Name: /opt/SAN16B/v5.1.0b/release.plist
Password:
Firmwaredownload has started.
...
Please avoid powering off the system during prom update.
...
Removing unneeded files, please wait ...
Finished removing unneeded files.

All packages have been downloaded successfully.
Firmwaredownload has completed successfully.
HA Rebooting ...
```

Again we are able to check the status using both the **`firmwaredownloadstatus`** and **`firmwareshow`** commands as can be seen in Example 1-32.

Example 1-32 Checking the firmware status on a SAN16B

```
IBM_2005_B16:admin> firmwaredownloadstatus
[1]: Wed Aug  2 22:41:07 2006
Firmware is being downloaded to the switch. This step may take up to 30
minutes.

[2]: Wed Aug  2 22:45:14 2006
Firmware has been downloaded to the secondary partition of the switch.

[3]: Wed Aug  2 22:46:36 2006
```

```
The firmware commit operation has started. This may take up to 10 minutes.

[4]: Wed Aug  2 22:49:23 2006
The commit operation has completed successfully.

[5]: Wed Aug  2 22:49:24 2006
Firmwaredownload command has completed successfully. Use firmwareshow to verify
the firmware versions.

IBM_2005_B16:admin> firmwareshow
Primary version:        v5.1.0b
Secondary version:      v5.1.0b
```

Staged upgrade to SAN256B switch using telnet

By implementing a staged upgrade to the firmware, we are able to both test the firmware upgrade and if required back out. Prior to upgrading using this method we must still complete all the preliminary preparation tasks, including running a **`configUpload`** of the switch.

We start by logging into the standby CP and run the **`firmwareDownload -s`** command as seen in Example 1-33 on page 264. This command uploads the firmware to the standby CP only and must be run on the standby CP.

Example 1-33 Firmwaredownload -s on the standby CP of a SAN256B

```
IBM_M48_SJC:admin> firmwareDownload -s
Server Name or IP Address: 10.64.209.228
FTP User Name: fm
File Name: /tempfos/v5.1.0c/release.plist
FTP Password:
Do Auto-Commit after Reboot [Y]: n
Reboot system after download [N]: Y
Firmware is being downloaded to the switch. This step may take up to 30
minutes.
Checking system settings for firmwaredownload...
Start to install packages...
dir                         ##################################################
ldconfig                    ##################################################
glibc                       ##################################################
...
lines deleted for clarity
...
fwdl                        ##################################################
swbd23-prom                 ##################################################
Please avoid powering off the system during prom update.
kernel                      ##################################################
sysklogd                    ##################################################
```

```
...
lines deleted for clarity
...
sysstat                     ##################################################
bpimage-swbd36              ##################################################
Writing kernel image into flash.
..............................
Finished writing kernel image.
Removing unneeded files, please wait ...
Finished removing unneeded files.

All packages have been downloaded successfully.
Firmware has been downloaded to the secondary partition of the switch.
```

The firmware download will cause the standby CP to reboot which will end our telnet session. We then log in to the primary CP, and run the **`haShow`** command to check the HA state of the director. It can take a few minutes for the standby CP to reboot and synchronize with the active CP.

> **Important:** If the CPs do not achieve synchronization you must log in to the standby CP and issue the firmwareRestore command to restore your original firmware.

When we have confirmed that the HA State is synchronized, we are ready to failover to the standby CP using the **`hafailover`** command as seen in Example 1-34.

Example 1-34 Failing over to the standby CP on a SAN256B director

```
IBM_M48_SJC:admin> hafailover
Local CP (Slot 6, CP1): Active, Warm Recovered
Remote CP (Slot 5, CP0): Standby, Healthy
HA enabled, Heartbeat Up, HA State synchronized

Warning: This command is being run on a redundant control
processor(CP) system. If the above status does not indicate
'HA State synchronized', then the CPs are not synchronized
and this operation will cause the active CP to reset. This
will cause disruption to devices attached to both switch 0
and switch 1 and will require that existing telnet sessions
be restarted. To reboot a single logical switch on this
system, use the switchreboot command while logged in to
that logical switch.

Are you sure you want to fail over to the standby CP [y/n]? y
Forcing Failover ...
```

Following the failover, we again check to see that the CPs synchronize, and also run the **`firmwareShow`** command again to confirm the current status. As we can see in Example 1-35, the primary partition on the active CP, CP0 is at firmware version v5.1.0c. However, the secondary partition of CP0 and both partitions on CP1 are still at v5.1.0b.

> **Note:** Observe that the two FR4-18i blades within our SAN256B director have also been upgraded to FOS v 5.1.0c, this is because they automatically synchronize to the firmware version of the active CP.

Example 1-35 Running firmwareShow during staged firmware upgrade - part1/2

```
IBM_M48_SJC:admin> firmwareShow
Slot Name      Primary/Secondary Versions              Status
---------------------------------------------------------------
  1  FR4-18i   v5.1.0c                                  Enabled
               v5.1.0c

  5  CP0       v5.1.0c                                  Active *
               v5.1.0b

  6  CP1       v5.1.0b                                  Standby
               v5.1.0b

 10  FR4-18i   v5.1.0c                                  Enabled
               v5.1.0c

*  Local CP

WARNING: The local CP and remote CP have different versions
of firmware, please retry firmwaredownload command.


********************************************************************
Notice: System has changed state to active.
All active commands are available now.
```

We can now log in to the standby CP - CP1 in our example and repeat the **`firmwareDownload -s`** process. When complete, we again run the **`firmwareShow command`** from the active CP. Our results are shown in Example 1-36.

Example 1-36 Running firmwareShow during staged firmware upgrade - part2/2

```
IBM_M48_SJC:admin> firmwareShow
Slot Name      Primary/Secondary Versions            Status
---------------------------------------------------------------
  1  FR4-18i   v5.1.0c                                Enabled
               v5.1.0c

  5  CP0       v5.1.0c                                Active *
               v5.1.0b

  6  CP1       v5.1.0c                                Standby
               v5.1.0b

 10  FR4-18i   v5.1.0c                                Enabled
               v5.1.0c
```

Both of the primary partitions on each of our CPs are now at the latest firmware level of v5.1.0c, and as such we can now complete any testing that we want to carry out before either backing out or committing the firmware. Notice that the secondary partitions for each CP still have the original firmware installed.

In order to complete the firmware upgrade, we can commit the firmware to each CP using the **`firmwareCommit`** command first on the standby and then on the active CP. Alternatively, in our example we show how to back out of the firmware upgrade by running the **`firmwareRestore`** command.

In Example 1-37 we log in to the standby CP and enter the **`firmwareRestore`** command.

Example 1-37 Restoring the previous firmware using the firmwareRestore command

```
login as: admin
admin@10.64.210.115's password:
*****************************************************************
Logging into STANDBY CP, not all commands are fully supported !!

IBM_M48_SJC:admin> firmwareRestore
Both primary and secondary partitions will be restored to the original firmware
after reboot.

The system is going down for reboot NOW !!

Broadcast message from root (pts/0) Fri Aug 18 21:33:24 2006...

The system is going down for reboot NOW !!
```

We then log back in to the standby CP and confirm the status using the **firmwaredownloadStatus** command as shown in Example 1-38.

Example 1-38 Checking the firmware download status

```
IBM_M48_SJC:admin> login as: admin
admin@10.64.210.115's password:
*****************************************************************
Logging into STANDBY CP, not all commands are fully supported !!
*****************************************************************

IBM_M48_SJC:admin> firmwaredownloadstatus
[1]: Fri Aug 18 21:00:38 2006
Slot 6 (CP1, standby): Firmware is being downloaded to the switch. This step
may take up to 30 minutes.

[2]: Fri Aug 18 21:14:33 2006
Slot 6 (CP1, standby): Firmware has been downloaded to the secondary partition
of the switch.

[3]: Fri Aug 18 21:33:08 2006
Slot 6 (CP1, standby): Firmwarerestore is entered. System will reboot and a
firmware commit operation will start upon boot up.

[4]: Fri Aug 18 21:34:13 2006
Slot 6 (CP1, standby): The firmware commit operation has started. This may take
up to 10 minutes.

[5]: Fri Aug 18 21:38:51 2006
Slot 6 (CP1, standby): The commit operation has completed successfully.

[6]: Fri Aug 18 21:38:51 2006
Slot 6 (CP1, standby): Firmwaredownload command has completed successfully. Use
firmwareshow to verify the firmware versions.
```

We then run a firmwareShow to verify the firmware versions. From Example 1-39 we can see that the Standby CP has been restored to FOS v5.1.0b.

Example 1-39 Running firmwareShow part way through firmware backout

```
IBM_M48_SJC:admin> firmwareShow
Slot Name      Primary/Secondary Versions              Status
---------------------------------------------------------------
  1  FR4-18i   v5.1.0c                                  Enabled
               v5.1.0c

  5  CP0       v5.1.0c                                  Active *
               v5.1.0b
  6  CP1       v5.1.0b                                 Standby
               v5.1.0b

 10  FR4-18i   v5.1.0c                                 Enabled
               v5.1.0c
...
```

output truncated for clarity

```
...
```

Note: The FR4-18i routing blade firmware status is only available on the Active CP. If we run **`firmwareShow`** from the Standby CP we will only see the details for the CPs themselves.

We can now failover to the Standby CP again using the **`haFailover`** command. When the HA state is synchronized, we can now log in to the new Standby CP - CP0 in our example, and repeat the **`firmwareRestore`** command. We can again watch this progress by using the **`firmwareDownloadStatus`** command. In Example 1-40 we can see the final report from the firmwareDownloadStatus command.

Example 1-40 Viewing the firmwareDownload status following firmwareRestore

```
IBM_M48_SJC:admin> firmwaredownloadstatus
```

...

lines deleted for clarity

...

```
[21]: Fri Aug 18 21:46:36 2006
Slot 5 (CP0, standby): Firmwarerestore is entered. System will reboot and a
firmware commit operation will start upon boot up.

[22]: Fri Aug 18 21:47:41 2006
Slot 5 (CP0, standby): The firmware commit operation has started. This may take
up to 10 minutes.

[23]: Fri Aug 18 21:52:19 2006
Slot 5 (CP0, standby): The commit operation has completed successfully.

[24]: Fri Aug 18 21:52:20 2006
Slot 5 (CP0, standby): Firmwaredownload command has completed successfully. Use
firmwareshow to verify the firmware versions.
```

Finally we run the **`firmwareShow`** command to see the final status as in Example 1-41.

Example 1-41 Firmware status following firmwareRestore

```
IBM_M48_SJC:admin> firmwareshow
Slot Name      Primary/Secondary Versions            Status
---------------------------------------------------------------
  1  FR4-18i   v5.1.0b                                Enabled
               v5.1.0b

  5  CP0       v5.1.0b                                Standby
               v5.1.0b

  6  CP1       v5.1.0b                                Active *
               v5.1.0b

 10  FR4-18i   v5.1.0b                                Enabled
               v5.1.0b
```

Notice that as the Active CP is now at v5.1.0b, the two router blades have also downloaded this firmware version. The firmware update to the router blades is considerably faster than that to the CPs due to the minimal OS that runs on them.

Troubleshooting a firmware upgrade

During our implementation we experienced a network failure to our ftp server which resulted in a failed firmware upgrade as detailed in Example 1-42.

Example 1-42 Firmware download failure

```
IBM_M48_SJC:admin> firmwareDownload
Server Name or IP Address: 10.64.209.228
FTP User Name: fm
File Name: /tempfos/v5.1.0c/release.plist
FTP Password:
The following AP blades are installed in the system.

Slot Name      Versions                         Traffic Disrupted
-----------------------------------------------------------------
  1  FR4-18i   v5.1.0b                                GigE
 10  FR4-18i   v5.1.0b                                GigE

This command will upgrade both CPs and all AP blade above. If
you want to upgrade a single CP only, please use -s option.

You can run firmwaredownloadstatus to get the status of this
command.

This command will cause the active CP to reset and will require
that existing telnet, secure telnet or SSH sessions be restarted.
```

```
Do you want to continue [Y]:
Firmware is being downloaded to standby CP. This step may take up to 30
minutes.

.
Firmware download failed on standby CP - Failed to download RPM package. Please
check the network connection. (0x15)
Remote CP is restoring its secondary partition.
Firmwarecommit has started on the remote CP. Please use firmwaredownloadstatus
and firmwareshow to see the firmware status.
```

Using **firmwareShow** and **firmwareDownloadStatus** we can see that the switch automatically recovered from this event as seen in Example 1-43.

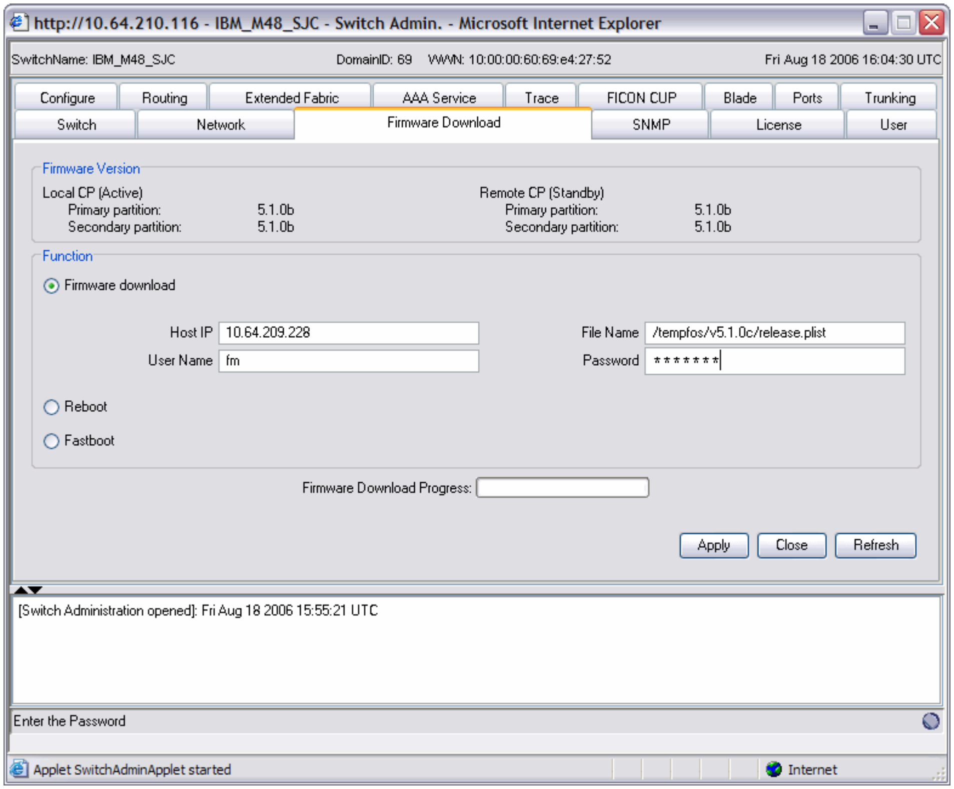
Example 1-43 Recovery from failed firmware update

```
IBM_M48_SJC:admin> firmwareShow
Slot Name      Primary/Secondary Versions              Status
---------------------------------------------------------------
  1  FR4-18i   v5.1.0b                                  Enabled
               v5.1.0b

  5  CP0       v5.1.0b                                  Active *
               v5.1.0b

  6  CP1       v5.1.0b                                  Standby
               v5.1.0b

 10  FR4-18i   v5.1.0b                                  Enabled
               v5.1.0b

IBM_M48_SJC:admin> firmwaredownloadstatus
[1]: Fri Aug 18 22:02:34 2006
Slot 5 (CP0, active): Firmware is being downloaded to standby CP. This step may
take up to 30 minutes.

[2]: Fri Aug 18 22:08:03 2006
Slot 5 (CP0, active): Firmware download failed on standby CP - Failed to
download RPM package. Please check the network connection. (0x15)

[3]: Fri Aug 18 22:08:57 2006
Slot 5 (CP0, active): Remote CP is restoring its secondary partition.

[4]: Fri Aug 18 22:08:58 2006
Slot 5 (CP0, active): Firmwarecommit has started on the remote CP. Please use
firmwaredownloadstatus and firmwareshow to see the firmware status.
```

After our ftp service is restored, we are then able to repeat the upgrade successfully.

Upgrading the firmware using the WebTools

As with upgrading the firmware using Telnet, we have to make sure that our FTP server is running, and that we have the server IP address. To upgrade the firmware using the WebTools, we point our Web browser to the IP address of the SAN switch. Next we click the **Admin button** to get into the Administration function. From there we navigate to the **Firmware Download tab** as shown in Figure 1-215.



http://10.64.210.116 - IBM_M48_SJC - Switch Admin. - Microsoft Internet Explorer

SwitchName: IBM_M48_SJC DomainID: 69 WWN: 10:00:00:60:69:e4:27:52 Fri Aug 18 2006 16:04:30 UTC

Firmware Version

Local CP (Active)
Primary partition: 5.1.0b
Secondary partition: 5.1.0b

Remote CP (Standby)
Primary partition: 5.1.0b
Secondary partition: 5.1.0b

Function

● Firmware download

Host IP: 10.64.209.228
User Name: fm
File Name: /tempfos/v5.1.0c/release.plist
Password: *******

○ Reboot

○ Fastboot

Firmware Download Progress:

[Switch Administration opened]: Fri Aug 18 2006 15:55:21 UTC

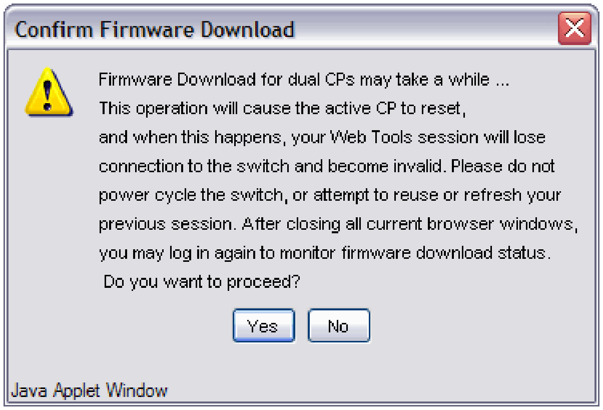
Enter the Password

Applet SwitchAdminApplet started

Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Blade
Ports
Trunking
Switch
Network
Firmware Download
SNMP
License
User
Apply
Close
Refresh
Internet

Figure 1-215 SAN-256B firmware download via WebTools

As mentioned earlier, we have to know the IP address of the host where we downloaded the firmware, the file name, user name, and password for logging in to the host. When these fields are filled in, we click **Apply**. We are prompted to confirm our actions as shown in Figure 1-216.



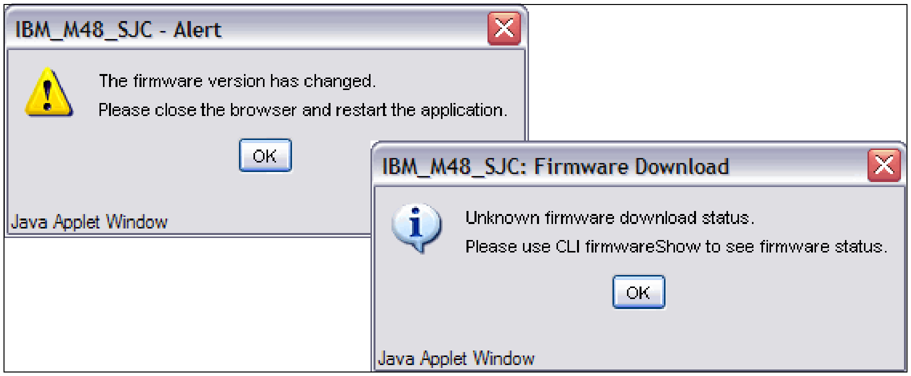
Firmware Download for dual CPs may take a while ...
This operation will cause the active CP to reset,
and when this happens, your Web Tools session will lose
connection to the switch and become invalid. Please do not
power cycle the switch, or attempt to reuse or refresh your
previous session. After closing all current browser windows,
you may log in again to monitor firmware download status.
Do you want to proceed?

Figure 1-216 Confirm firmware download

Tip: While performing the firmware upgrade, we recommend that you take advantage of your scheduled fabric outage and enable the core PID setting if it is not already set. Refer to “Setting Core PID format” on page 54 to enable it using WebTools.

The download begins. Status messages are logged in the report window. There is also a Firmware download status indicator which shows the progress.

When the download completes and both CPs have been rebooted, we receive a message indicating that we have to shut down all WebTools and browser windows and restart the WebTools, see Figure 1-217.



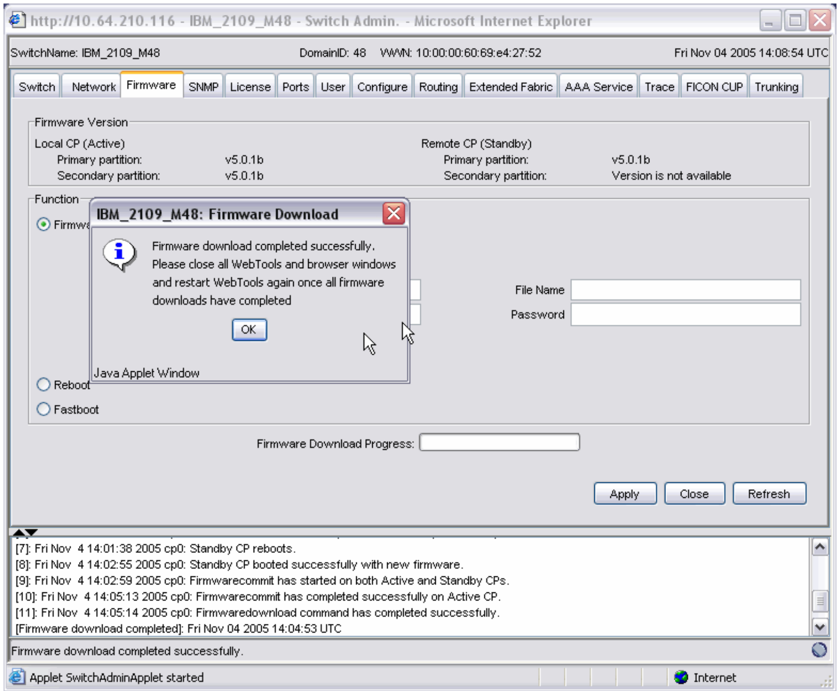
The firmware version has changed.
Please close the browser and restart the application.

Unknown firmware download status.
Please use CLI firmwareShow to see firmware status.

Figure 1-217 SAN256B firmware upgrade alerts

If the WebTools session is not lost during the upgrade, we can also see the completion messages in the report window in Figure 1-218.

Our firmware update using WebTools is now complete.


http://10.64.210.116 - IBM_2109_M48 - Switch Admin. - Microsoft Internet Explorer
Switch
Network
Firmware
SNMP
License
Ports
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Trunking
Function
Reboot
Fastboot
File Name
Password
Firmware Download Progress:
Apply
Close
Refresh
IBM_2109_M48: Firmware Download
OK
Java Applet Window
Applet SwitchAdminApplet started
Internet

SwitchName: IBM_2109_M48 DomainID: 48 WWN: 10:00:00:60:69:e4:27:52 Fri Nov 04 2005 14:08:54 UTC

Firmware Version

Local CP (Active)
Primary partition: v5.0.1b
Secondary partition: v5.0.1b

Remote CP (Standby)
Primary partition: v5.0.1b
Secondary partition: Version is not available

Firmware download completed successfully. Please close all WebTools and browser windows and restart WebTools again once all firmware downloads have completed

```
[7]: Fri Nov  4 14:01:38 2005 cp0: Standby CP reboots.
[8]: Fri Nov  4 14:02:55 2005 cp0: Standby CP booted successfully with new firmware.
[9]: Fri Nov  4 14:02:59 2005 cp0: Firmwarecommit has started on both Active and Standby CPs.
[10]: Fri Nov  4 14:05:13 2005 cp0: Firmwarecommit has completed successfully on Active CP.
[11]: Fri Nov  4 14:05:14 2005 cp0: Firmwaredownload command has completed successfully.
[Firmware download completed]: Fri Nov 04 2005 14:04:53 UTC
```

Firmware download completed successfully.

Figure 1-218 SAN256B firmware download complete via WebTools

Note: The name server might not be available for a few minutes after upgrading your switch firmware. This is expected behavior.

1.9.8 Advanced Security

To implement a secure fabric on an IBM TotalStorage SAN Switch, we require two things: an optional Advanced Security (AS) license key, and a firmware version supporting Secure Fabric OS (SFOS). When installed and configured, it provides a comprehensive SAN security solution for IBM 2109 and 2005 switches and the devices that are attached to them. All IBM 2109 and 2005 switch models are supported, and can be used in a mixed environment.

Note: IBM has OEM'd Brocade's Secure Fabric OS, and the IBM name for this product is *Advanced Security.* At some stages throughout this topic, we interchange the nomenclature.

Features

Advanced Security provides the ability to:

- Secure the SAN infrastructure from unauthorized management and device access.
- Share resources within the same fabric by tightly controlling where devices (servers / hosts) can attach.
- Provide a secure means for distributing fabric wide security and zoning information (trusted switch).
- Create a "trusted SAN infrastructure".

Control

The security level for the fabric is defined by a Fabric Management Policy Set (FMPS) that consists of:

- Fabric Configuration Server (FCS) policy
- Management Access Control (MAC) policies
- Device Connection Control (DCC) policies
- Switch Connection Control (SCC) policy
- Options policy (prevents Node WWN usage)

Management

To manage an Advanced Security environment, we can use Telnet, Fabric Manager, or API integration into SAN Management software, such as Tivoli SAN Manager.

Planning

Before we leap ahead and enable security on our fabric, we have to do some planning to minimize any disruption to our SAN services:

- Document the switch name, WWN, and IP address of every switch in the fabric(s).
- Identify which switches will be the Fabric Configuration Server (FCS), and also identify at least one to be the backup FCS.
- Determine the policy requirements for each device and host.
- Identify management workstations to install secure Telnet or SSH client on.

- All switches must have minimum firmware levels to support SFOS as listed in Table 1-8 on page 39.
- All switches in the fabric must have a zoning and security license.
- Digital certificates must be installed on each switch in the fabric before enabling security.

> **Note:** Only switches *upgraded* to v2.6.1, v3.1 and v4.1 firmware will require digital certificates to be added. All new switches shipped with these levels of firmware pre-installed will already have the digital certificates loaded.

Implementing Advanced Security

We now perform the steps to implement security on our fabric, assuming that we have completed upgrading firmware to the required levels by following the procedure in 1.9.7, “Upgrading the switch” on page 254. We also assume that the security license key has been purchased and installed on all switches in the fabric.

The first step we perform is to back up the configuration of all the switches in our fabric. This is an important step that allows us to be able to restore the switch to its current condition if anything should go wrong during our implementation process. To do this, we follow the procedures outlined in “Upload/download” on page 144 for each switch, ensuring that we select the **Config Upload** option. This can also be accomplished using the **`configUpload`** command in a telnet session.

Our next step is to determine if digital certificates are installed on our switches in the fabric. We perform this on all switches by using the **`pkishow`** command as follows (Example 1-44).

Example 1-44 Checking the certificate status using pkishow

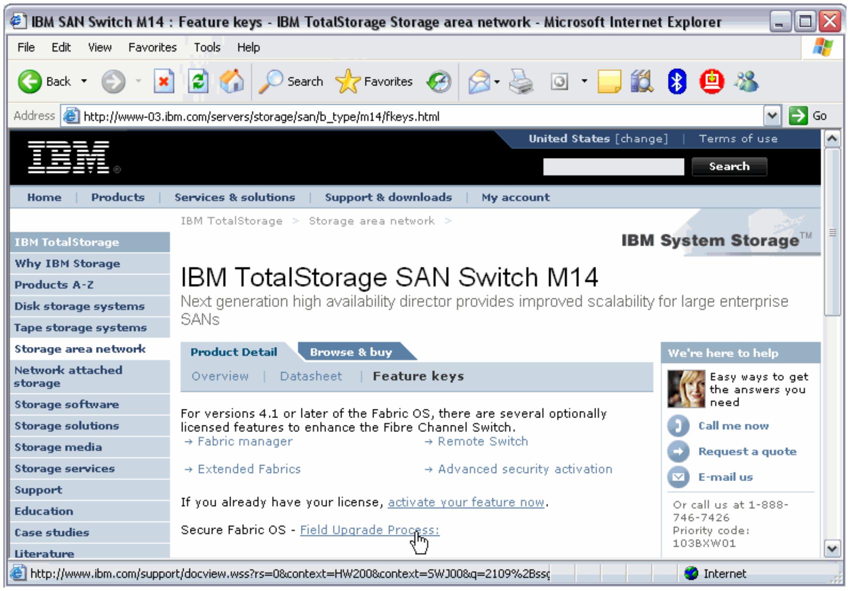
```
ITSO_2005_B32:admin> pkishow
Passphrase       : Exist
Private Key      : Exist
CSR              : Exist
Certificate      : Empty
Root Certificate: Exist
```

We can see that the Certificate shows as *Empty*, therefore we have to install this. We perform this action for a SAN-16B, although the procedure is the same on all switch models.

We visit the IBM TotalStorage SAN Switch Web site at:

`http://www-1.ibm.com/servers/storage/san/b_type/index.html`

From this Web site, we select the model of the switch we are working with. In our example, we have selected the SAN switch M12. From the displayed Web page, we now select the **Feature Keys** tab, which allows you to select the Field Upgrade Process for the Secure Fabric OS upgrade as seen in Figure 1-219.


IBM SAN Switch M14 : Feature keys - IBM TotalStorage Storage area network - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://www-03.ibm.com/servers/storage/san/b_type/m14/fkeys.html
Go
IBM
United States [change]
Terms of use
Search
Home
Products
Services & solutions
Support & downloads
My account
IBM TotalStorage
Storage area network
IBM System Storage™
IBM TotalStorage
Why IBM Storage
Products A-Z
Disk storage systems
Tape storage systems
Storage area network
Network attached storage
Storage software
Storage solutions
Storage media
Storage services
Support
Education
Case studies
Literature
Product Detail
Browse & buy
Overview
Datasheet
Feature keys
We're here to help
Call me now
Request a quote
E-mail us
http://www.ibm.com/support/docview.wss?rs=0&context=HW200&context=SWJ00&q=2109%2Bssc
Internet

IBM TotalStorage SAN Switch M14

Next generation high availability director provides improved scalability for large enterprise SANs

For versions 4.1 or later of the Fabric OS, there are several optionally licensed features to enhance the Fibre Channel Switch.

→ Fabric manager
→ Remote Switch
→ Extended Fabrics
→ Advanced security activation

If you already have your license, activate your feature now.

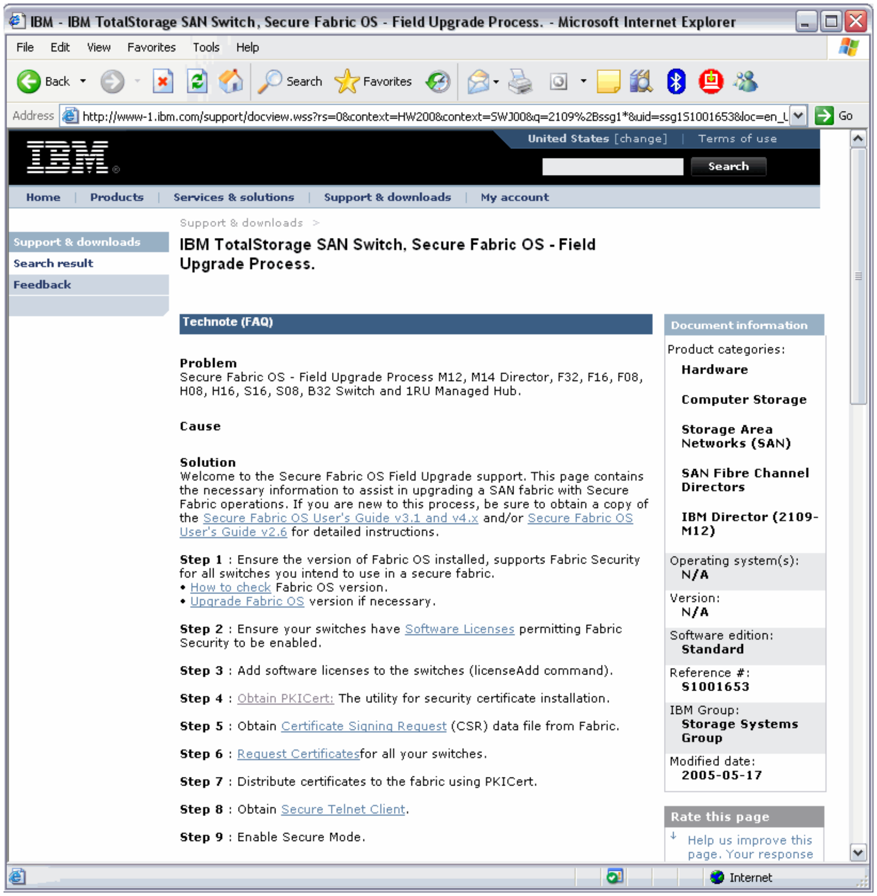
Secure Fabric OS - Field Upgrade Process:

Easy ways to get the answers you need

Or call us at 1-888-746-7426
Priority code: 103BXW01

Figure 1-219 M14 certificate download

After we select the field upgrade process, we can then select **Obtain PKI Certificate** as shown in Figure 1-220.


IBM - IBM TotalStorage SAN Switch, Secure Fabric OS - Field Upgrade Process. - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://www-1.ibm.com/support/docview.wss?rs=0&context=HW200&context=SWJ00&q=2109%2Bssg1*&uid=ssg1S1001653&loc=en_U
Go
United States [change]
Terms of use
Search
Home
Products
Services & solutions
Support & downloads
My account
Support & downloads
Search result
Feedback
Support & downloads >
Internet

IBM TotalStorage SAN Switch, Secure Fabric OS - Field Upgrade Process.

Technote (FAQ)

Problem
Secure Fabric OS - Field Upgrade Process M12, M14 Director, F32, F16, F08, H08, H16, S16, S08, B32 Switch and 1RU Managed Hub.

Cause

Solution
Welcome to the Secure Fabric OS Field Upgrade support. This page contains the necessary information to assist in upgrading a SAN fabric with Secure Fabric operations. If you are new to this process, be sure to obtain a copy of the Secure Fabric OS User's Guide v3.1 and v4.x and/or Secure Fabric OS User's Guide v2.6 for detailed instructions.

Step 1 : Ensure the version of Fabric OS installed, supports Fabric Security for all switches you intend to use in a secure fabric.
- How to check Fabric OS version.
- Upgrade Fabric OS version if necessary.

Step 2 : Ensure your switches have Software Licenses permitting Fabric Security to be enabled.

Step 3 : Add software licenses to the switches (licenseAdd command).

Step 4 : Obtain PKICert: The utility for security certificate installation.

Step 5 : Obtain Certificate Signing Request (CSR) data file from Fabric.

Step 6 : Request Certificatesfor all your switches.

Step 7 : Distribute certificates to the fabric using PKICert.

Step 8 : Obtain Secure Telnet Client.

Step 9 : Enable Secure Mode.

Document information

Product categories:
Hardware
Computer Storage
Storage Area Networks (SAN)
SAN Fibre Channel Directors
IBM Director (2109-M12)

Operating system(s):
N/A

Version:
N/A

Software edition:
Standard

Reference #:
S1001653

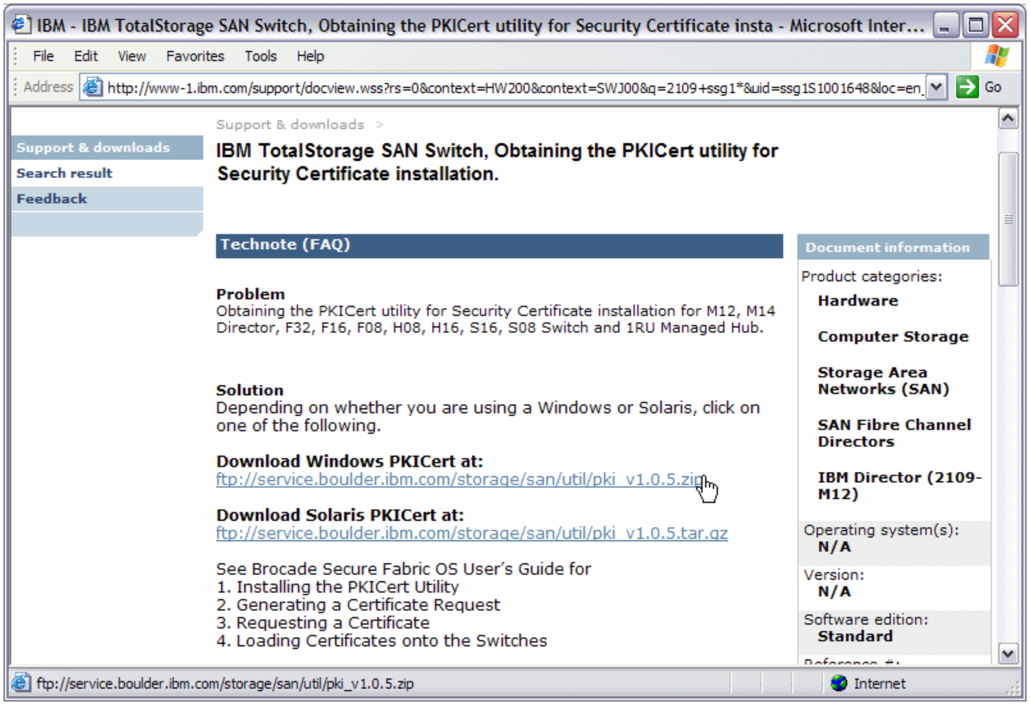
IBM Group:
Storage Systems Group

Modified date:
2005-05-17

Rate this page
Help us improve this page. Your response

Figure 1-220 Field Upgrade Process Web Page

From here we are directed to the site where we can download the PKICert utility. We are presented with two options, one for Windows and one for Solaris. In the example shown in Figure 1-221, we selected the option to download the Windows certificate.


IBM - IBM TotalStorage SAN Switch, Obtaining the PKICert utility for Security Certificate insta - Microsoft Inter...
File Edit View Favorites Tools Help
Address http://www-1.ibm.com/support/docview.wss?rs=0&context=HW200&context=SWJ00&q=2109+ssg1*&uid=ssg1S1001648&loc=en_
Go
Support & downloads >
Support & downloads
Search result
Feedback
Technote (FAQ)
Document information
ftp://service.boulder.ibm.com/storage/san/util/pki_v1.0.5.zip
Internet

IBM TotalStorage SAN Switch, Obtaining the PKICert utility for Security Certificate installation.

Problem
Obtaining the PKICert utility for Security Certificate installation for M12, M14 Director, F32, F16, F08, H08, H16, S16, S08 Switch and 1RU Managed Hub.

Solution
Depending on whether you are using a Windows or Solaris, click on one of the following.

Download Windows PKICert at:
ftp://service.boulder.ibm.com/storage/san/util/pki_v1.0.5.zip

Download Solaris PKICert at:
ftp://service.boulder.ibm.com/storage/san/util/pki_v1.0.5.tar.gz

See Brocade Secure Fabric OS User's Guide for
1. Installing the PKICert Utility
2. Generating a Certificate Request
3. Requesting a Certificate
4. Loading Certificates onto the Switches

Product categories:
Hardware
Computer Storage
Storage Area Networks (SAN)
SAN Fibre Channel Directors
IBM Director (2109-M12)

Operating system(s):
N/A

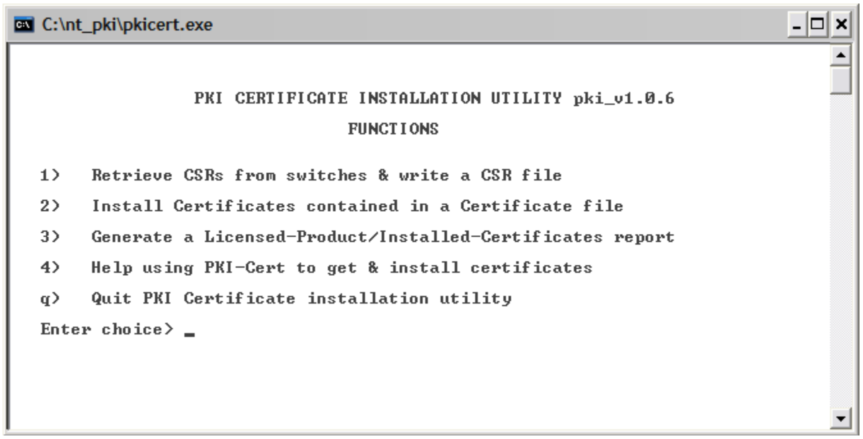
Version:
N/A

Software edition:
Standard

Figure 1-221 Download Windows security certificate

At the time of writing, these Web pages are being updated to include a link to the latest version of the PKI Cert utility. As such, we have downloaded v1.0.6 and proceeded with this.

We extract the zip file to a temporary directory, where we can then run the Setup.exe to install the utility on our workstation. During the install process, we select all the default options. When the install completes, we run **`c:\nt_pki\pkicert.exe`**. After this opens, we press Enter to accept the default log file, and are then presented with the menu shown in Figure 1-222.



```
                PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6
                                FUNCTIONS

 1>   Retrieve CSRs from switches & write a CSR file
 2>   Install Certificates contained in a Certificate file
 3>   Generate a Licensed-Product/Installed-Certificates report
 4>   Help using PKI-Cert to get & install certificates
 q>   Quit PKI Certificate installation utility
 Enter choice> _
```

Figure 1-222 PKI Cert Utility menu

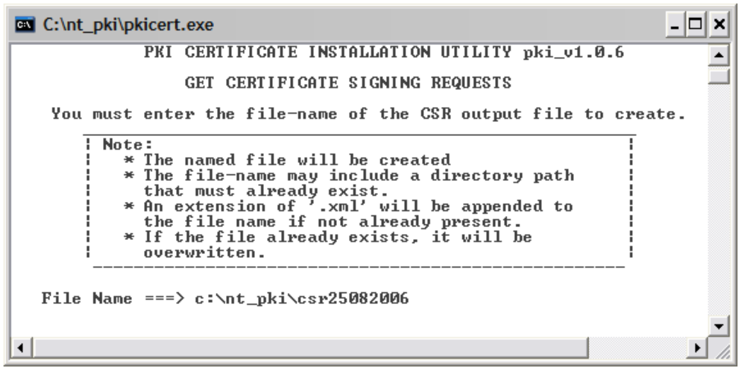
Obtain CSRs

From the menu we take option **1**, to retrieve CSRs from switches and write a CSR file. This takes us to another menu where we are given the following options:

```
1)   Manually enter fabric address
2)   Read addresses from a file (name to be given)
r)   Return to Main menu
```

We take option **1** to allow us to manually enter our fabric’s address. From the next window, we only have to enter an IP address of one switch within a fabric, we can enter multiple fabrics if we want, and by just pressing Enter without entering an address on a line, continue to the next window.

At this point the PKI Cert utility connects to the fabric, and prompts us for the userid and password (we are given five attempts). The next window prompts us for a file name as shown in Figure 1-223 on page 281, where we enter a fully qualified file name and path where we would like to store the CSR information from the fabric switches.

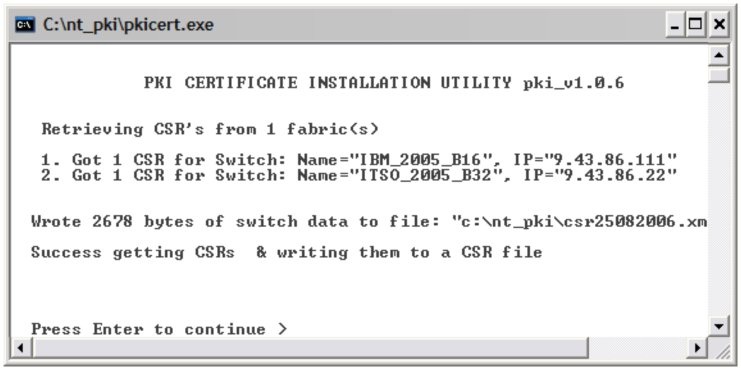


```
            PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6

                GET CERTIFICATE SIGNING REQUESTS

    You must enter the file-name of the CSR output file to create.
          _______________________________________________________
          | Note:                                                |
          |   * The named file will be created                   |
          |   * The file-name may include a directory path       |
          |     that must already exist.                         |
          |   * An extension of '.xml' will be appended to       |
          |     the file name if not already present.            |
          |   * If the file already exists, it will be           |
          |     overwritten.                                     |
           -----------------------------------------------------

   File Name ===> c:\nt_pki\csr25082006
```

Figure 1-223 PKI CSR file name

After entering the file name, we are asked if we would like to Include (optional) licensed product data; we replied `Yes` to save the optional data. We are then asked if we want to get CSRs from switches that already have certificates. As our aim here is to install certificates on switches without them currently, we answer `No` to this question.

Next we are asked which fabric we want to retrieve from; we selected all. Now the utility retrieves the CSRs from each switch, giving us its progress as shown in Figure 1-224.



```
            PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6

   Retrieving CSR's from 1 fabric(s)

   1. Got 1 CSR for Switch: Name="IBM_2005_B16", IP="9.43.86.111"
   2. Got 1 CSR for Switch: Name="ITSO_2005_B32", IP="9.43.86.22"

  Wrote 2678 bytes of switch data to file: "c:\nt_pki\csr25082006.xm

  Success getting CSRs  & writing them to a CSR file


  Press Enter to continue >
```

Figure 1-224 PKI Certificate retrieval status

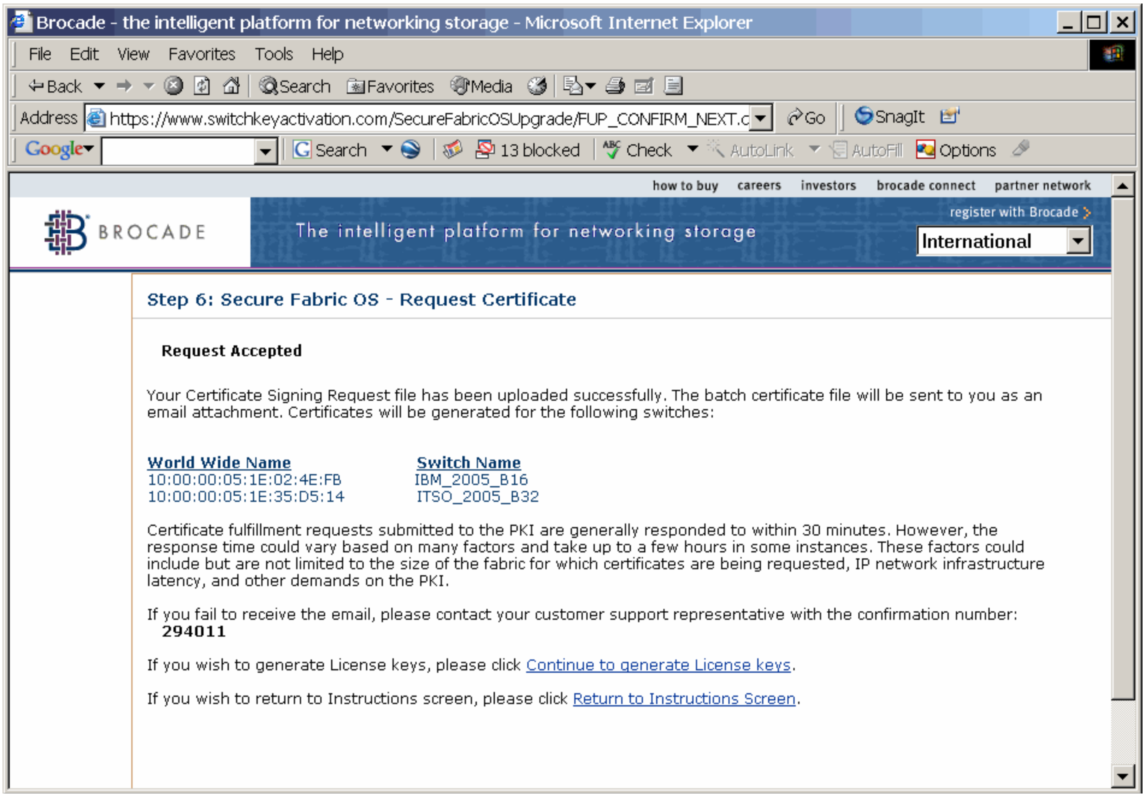
When this completes, we press Enter to continue. This returns us to the first menu, where we select **q** to quit.

Request certificates

Now that we have saved the CSR file on our workstation, we return to step 6 on the Field Upgrade process Web page, as shown in Figure 1-220 on page 278.

We click the **Request Certificates** link at step 6, and are taken to the Brocade switch key activation site. After agreeing to the licensing, and filling out our details, we point the browser to the CSR file we saved from the switches in the previous steps, and click the **Submit** button. We verify our information and click **Submit** again.

Figure 1-225 shows the request certificate confirmation.


Brocade - the intelligent platform for networking storage - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://www.switchkeyactivation.com/SecureFabricOSUpgrade/FUP_CONFIRM_NEXT.c
Go SnagIt
Google Search 13 blocked Check AutoLink AutoFill Options
how to buy careers investors brocade connect partner network
BROCADE
The intelligent platform for networking storage
register with Brocade
International

Step 6: Secure Fabric OS - Request Certificate

Request Accepted

Your Certificate Signing Request file has been uploaded successfully. The batch certificate file will be sent to you as an email attachment. Certificates will be generated for the following switches:

World Wide Name	Switch Name
10:00:00:05:1E:02:4E:FB	IBM_2005_B16
10:00:00:05:1E:35:D5:14	ITSO_2005_B32

Certificate fulfillment requests submitted to the PKI are generally responded to within 30 minutes. However, the response time could vary based on many factors and take up to a few hours in some instances. These factors could include but are not limited to the size of the fabric for which certificates are being requested, IP network infrastructure latency, and other demands on the PKI.

If you fail to receive the email, please contact your customer support representative with the confirmation number:
294011

If you wish to generate License keys, please click Continue to generate License keys.

If you wish to return to Instructions screen, please click Return to Instructions Screen.

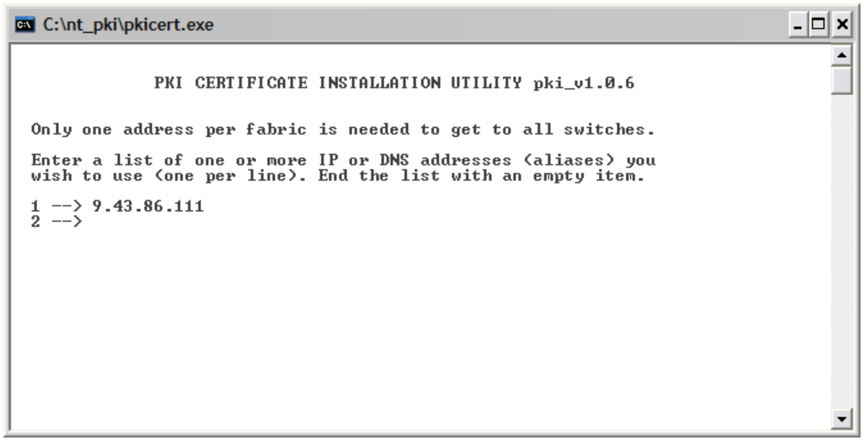
Figure 1-225 Brocade Request Certificate confirmation

After we have submitted our collected file, an automated machine will process it, shortly after we have received the digital certificates at the e-mail address we provided in the submit form. We detach the certificates file to a temporary directory, and execute the **`c:\nt_pki\pkicert.exe`** utility again.

> **Note:** If the CSR collected includes a switch without a Security license, the submitted CSR file will not be processed.

Install the certificates

This time, from the PKICert utility menu shown in Figure 1-222 on page 280, we select option **2** to Install Certificates contained in the Certificate file we received. We then select option **1** to Manually enter the fabric IP address. We show the IP address entry here in Figure 1-226, where pressing Enter on the second line (instead of supplying another IP address) advances us to the next window.

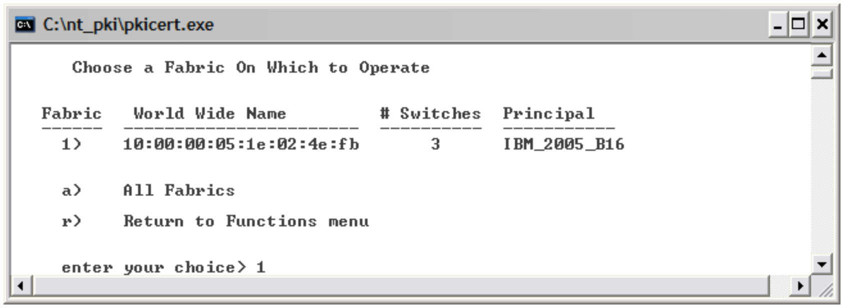


```
            PKI CERTIFICATE INSTALLATION UTILITY pki_v1.0.6

  Only one address per fabric is needed to get to all switches.

  Enter a list of one or more IP or DNS addresses (aliases) you
  wish to use (one per line). End the list with an empty item.

  1 --> 9.43.86.111
  2 -->
```

Figure 1-226 IP address input

At this point we are asked to provide the login *user* and *password* for PKICert to connect to the fabric. After PKICert successfully connects to the fabric, we are prompted for the full path and file name of the Certificate file we received in the e-mail earlier.

Next we select the target fabric as shown in Figure 1-227.

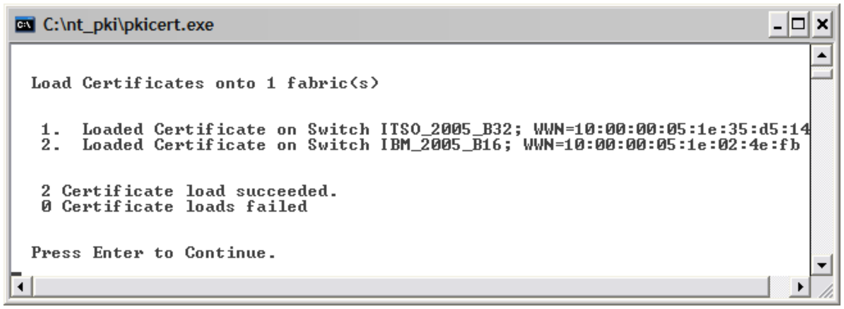


```
     Choose a Fabric On Which to Operate

   Fabric   World Wide Name         # Switches  Principal
   ------  -----------------------  ----------  -----------
     1>    10:00:00:05:1e:02:4e:fb       3      IBM_2005_B16

     a)    All Fabrics

     r)    Return to Functions menu

     enter your choice> 1
```

Figure 1-227 Target fabric selection

If we had entered multiple fabric IP addresses earlier, we could now select an individual fabric or all the fabrics listed. In our case, we have only entered a single fabric.

The utility now installs the certificates on each switch in the fabric, confirming the success or failure as displayed in Figure 1-228.



```
Load Certificates onto 1 fabric(s)

 1.  Loaded Certificate on Switch ITSO_2005_B32; WWN=10:00:00:05:1e:35:d5:14
 2.  Loaded Certificate on Switch IBM_2005_B16; WWN=10:00:00:05:1e:02:4e:fb

 2 Certificate load succeeded.
 0 Certificate loads failed

Press Enter to Continue.
```

Figure 1-228 Certificate installation success

After pressing Enter to continue, we select **q** to quit the PKICert Utility.

We now confirm that we have successfully installed the digital certificates by issuing **`pkishow`** command for v4.1 and above as seen in Example 1-45.

Example 1-45 Confirming that digital certificates have been successfully installed

```
ITSO_2005_B32:admin> pkishow
Passphrase      : Exist
Private Key     : Exist
CSR             : Exist
Certificate     : Exist
Root Certificate: Exist
ITSO_2005_B32:admin>
```

How to telnet to a switch securely

Now that we have successfully installed the digital certificates on all our switches, we have to prepare our workstation to be able to securely communicate with the FCS switches in the fabric once we enable security, because normal telnet will not be allowed to connect.

From step 8 in the Web page shown in Figure 1-220 on page 278, we click the link, **Obtain Secure Telnet Client**, to download the client. We are taken to another Web page where we can select a Windows or Solaris client. We selected the Windows download link and saved *ntsectelnet.zip* to our workstation.

We then unzip the file, making sure we maintain the directory structure (if the directory structure is not maintained, the install will fail).

From our temporary unzip location, we then execute **`setup.exe`** (Figure 1-229).

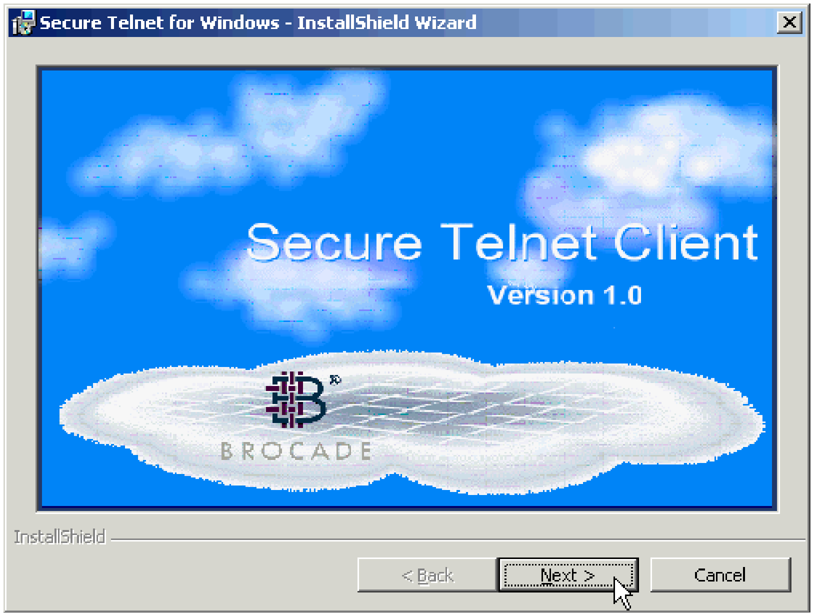
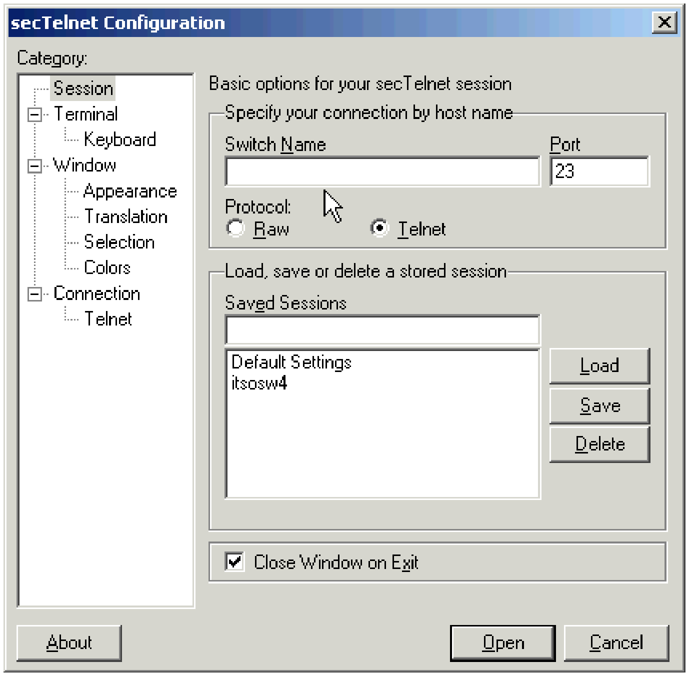

Secure Telnet for Windows - InstallShield Wizard
Secure Telnet Client
Version 1.0
BROCADE
InstallShield
< Back
Next >
Cancel

Figure 1-229 Secure Telnet Install

Figure 1-229 shows the Install shield splash window for the Brocade Secure Telnet client installer. We click the **Next** button to install the client with all default values and complete the install process. This puts a Secure Telnet Icon on our desktop. We double-click this icon to open the window shown in Figure 1-230.


secTelnet Configuration
Category:
Session
Terminal
Keyboard
Window
Appearance
Translation
Selection
Colors
Connection
Telnet
Basic options for your secTelnet session
Specify your connection by host name
Load, save or delete a stored session
Load
Save
Delete
About
Open
Cancel

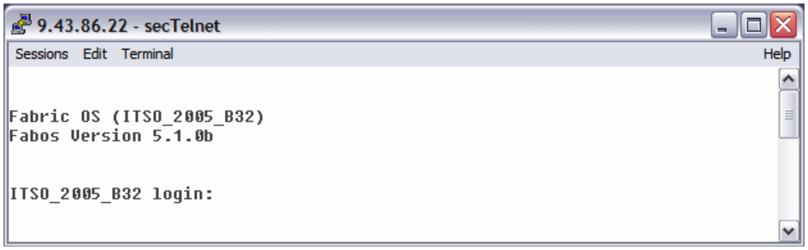
Switch Name
Port 23
Protocol: ○ Raw ● Telnet

Saved Sessions
Default Settings
itsosw4

☑ Close Window on Exit

Figure 1-230 Secure Telnet client configuration

In this secTelnet Configuration window, we enter the IP address of the FCS switch we want to connect to in the Switch Name field, and then click the **Open** button. We also have an option of saving the connection definition, by entering a name in the Saved Sessions field and clicking the **Save** button. In our example, we have saved a session for the itsosw4 switch. Now, by double-clicking the name, we launch a secure Telnet session to that switch, as shown in Figure 1-231.


9.43.86.22 - secTelnet
Sessions
Edit
Terminal
Help

```
Fabric OS (ITSO_2005_B32)
Fabos Version 5.1.0b


ITSO_2005_B32 login:
```

Figure 1-231 Secure Telnet session

As the secure Telnet session uses the digital certificates that we have previously installed on the switch, establishing a connection verifies that we are ready to begin enabling Advanced Security.

Tip: Before enabling Advanced Security on the fabric, we recommend performing the secure Telnet session establishment to each switch in the fabric to verify that the certificates are working properly before we lock the fabric with security policies.

Enabling Advanced Security

Before continuing, we recommend performing a backup of the configuration of all the switches in our fabric again. This lets us restore the switch to this checkpoint in the procedure, if all is well currently. To do this, we follow the procedures outlined in “Upload/download” on page 144, ensuring that we select the **Config Upload** option. This can also be accomplished using the **`configUpload`** command in a telnet session. If a restore of these saved configurations is required, this can be accomplished using the **`configDownload`** command.

Tip: Using different **`configUpload`** save names ensures that we have two different restore points.

We have now prepared our fabric for Advanced Security; also, during our planning step, we have identified which switches we intend to make the Primary and Backup FCSs. To continue, we have to schedule a fabric outage, because enabling Advanced Security is a fabric-wide setting, and causes all switches in the fabric to reboot.

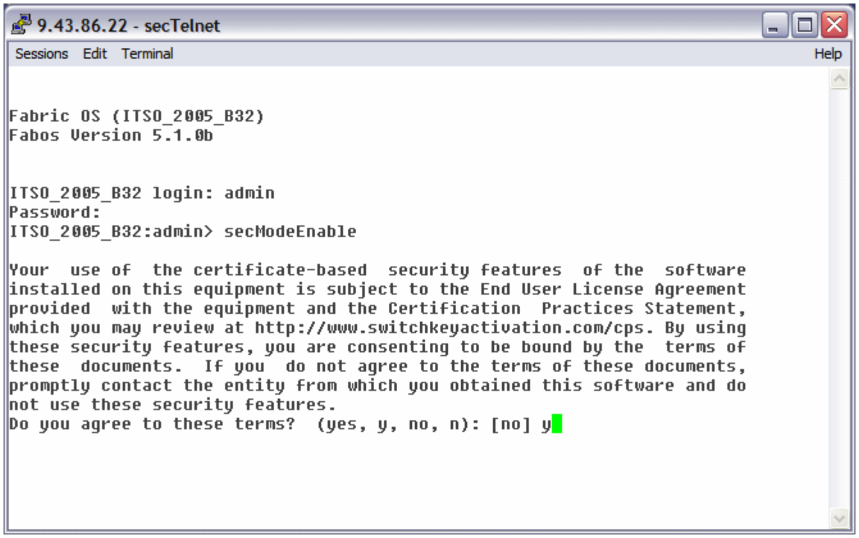
Enabling secure mode:

- Creates a default Fabric Management Policy Set (FMPS) using the FCS policy containing the WWNs that are specified in the list
- Distributes the FMPS to all switches in the fabric
- Activates the FMPS
- Reboots all switch systems (Note: The switches themselves do not reboot)

The Primary FCS switch:

- Distributes the default policy sets to all switches in the fabric
- Activates the zoning configurations and any future zone management
- Applies the FMPS policy set

Using the secTelnet client we installed earlier, we now connect to the switch we have identified as being our Primary FCS. After logging in to the switch, we use the **`secModeEnable`** command as shown in Figure 1-232, where we must read and agree to the End User License Agreement.



```
Fabric OS (ITSO_2005_B32)
Fabos Version 5.1.0b


ITSO_2005_B32 login: admin
Password:
ITSO_2005_B32:admin> secModeEnable

Your  use of  the certificate-based  security features  of the  software
installed on this equipment is subject to the End User License Agreement
provided  with the equipment and the Certification  Practices Statement,
which you may review at http://www.switchkeyactivation.com/cps. By using
these security features, you are consenting to be bound by the  terms of
these  documents.  If you  do not agree to the terms of these documents,
promptly contact the entity from which you obtained this software and do
not use these security features.
Do you agree to these terms?  (yes, y, no, n): [no] y
```

Figure 1-232 The secModeEnable command

We enter **y** to agree to the terms. Next we are asked to define the FCS list; at a minimum, we recommend defining two separate switches as FCS. One switch operates as the primary Fabric Configuration Server and the other as backup, in case the primary were ever to fail. More FCS switches can be defined, although we do recommend that these switches also be located in a physically secure environment.

The following Example 1-46 shows how we defined a SAN32B and the SAN16B in our fabric as FCS switches:

Example 1-46 Defining FCS switches using secModeEnable

```
This command requires Switch Certificate,  Security license and Zoning license
to be installed on  every switch in the fabric.

PLEASE NOTE: On successful completion of this command, login sessions may be
closed and some switches may go through a reboot to form a secure fabric.

This is an interactive session to create a FCS list.

The new FCS list is empty.

Enter WWN, Domain, or switch name(Leave blank when done): ITSO_2005_B32
Switch WWN is 10:00:00:05:1e:35:d5:14.

The new FCS list:
  10:00:00:05:1e:35:d5:14
```

```
Enter WWN, Domain, or switch name(Leave blank when done): IBM_2005_B16
Switch WWN is 10:00:00:05:1e:02:4e:fb.

The new FCS list:
  10:00:00:05:1e:35:d5:14
  10:00:00:05:1e:02:4e:fb

Enter WWN, Domain, or switch name(Leave blank when done):
Are you done?  (yes, y, no, n): [no] y
```

In our example we defined the FCS switches by entering their switch names; we could also define them by entering their domain ID, or WWN.

The process continues by prompting us to change the current passwords, which include:

- Root password for the FCS switch
- Factory password for the FCS switch
- Admin password for the FCS switch
- User password for the fabric
- Admin password for the non-FCS switches

The following coding shows the prompts to define each of these passwords. Also shown is the case where we entered a password that was too short; passwords must be between 8 and 40 characters in length:

```
Please enter current admin account password:
Changing password for root
New FCS switch root password:
Password must be between 8 and 40 characters long.
New FCS switch root password:
Re-type new password:
Changing password for factory
New FCS switch factory password:
Re-type new password:
Changing password for admin
New FCS switch admin password:
You cannot reuse the old password.
New FCS switch admin password:
Re-type new password:
Changing password for user
New fabric wide user password:
Re-type new password:
Changing password for admin
New Non FCS switch admin password:
Re-type new password:
```

After entering the last password verification, all switches in the fabric reconfigure with advanced security in place. When the system reboots are complete, the fabric is now secured using default policies.

With the secure fabric now enabled, we are only able to manage the fabric from the FCS switches.

If we are running FCS switches that have v4.1 or higher firmware, we can secure our fabric further by disabling the telnet daemon to our FCS switches, only allowing SSH sessions to be established. Be aware that SSH is supported from v4.1 whether or not Secure Fabric OS is licensed. To disable the telnet interface, we use **`secTelnet`** to our FCS switch and run the **`configure`** command as seen in Example 1-47.

> **Note:** The **`configure`** command on a secure FCS switch does not require the switch to be disabled as it normally is in a non-secure or non-FCS switch, and only presents specific options that can be changed concurrently.

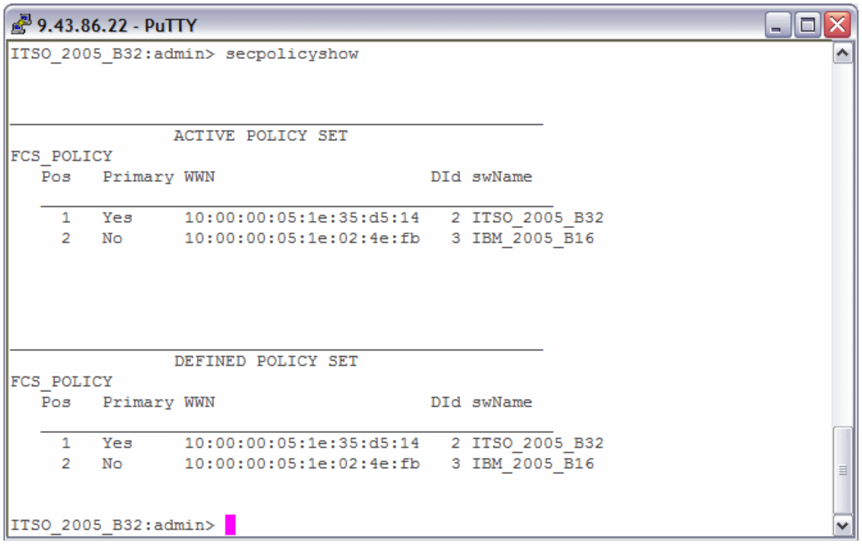
Example 1-47 Using configure to disable telnet

```
ITSO_2005_B32:admin> configure

Not all options will be available on an enabled switch.
To disable the switch, use the "switchDisable" command.

Configure...

  System services (yes, y, no, n): [no] y

    rstatd (on, off): [off]
    rusersd (on, off): [off]
    telnetd (on, off): [on] off
  ssl attributes (yes, y, no, n): [no]
  http attributes (yes, y, no, n): [no]
  snmp attributes (yes, y, no, n): [no]
  rpcd attributes (yes, y, no, n): [no]
  cfgload attributes (yes, y, no, n): [no]
  webtools attributes (yes, y, no, n): [no]

ITSO_2005_B32:admin>
```

As we have now disabled the telnetd daemon completely, we are only able to use an SSH client to connect to the switch. An example of an SSH client is PuTTY, which can be freely downloaded from the Internet.

Some other useful commands to view and manage the security policies are:

- **`secPolicyFcsRemove`**: Used to change the position of a switch in the FCS list.
- **`secFcsFailover`**: Used to cause the primary FCS switch to failover to the next FCS switch in the list.
- **`secPolicyAdd`**: Used to add members to a specified policy.
- **`secPolicyRemove`**: Used to remove a member from a specified policy.
- **`secPolicyShow`**: Displays a list of current FCS switches and identifies the primary. The output of **`secPolicyShow`** for our fabric is shown in Figure 1-233.



```
ITSO_2005_B32:admin> secpolicyshow



____________________________________________________
                ACTIVE POLICY SET
FCS_POLICY
   Pos   Primary WWN                     DId swName
   __________________________________________________
     1   Yes     10:00:00:05:1e:35:d5:14   2 ITSO_2005_B32
     2   No      10:00:00:05:1e:02:4e:fb   3 IBM_2005_B16





____________________________________________________
                DEFINED POLICY SET
FCS_POLICY
   Pos   Primary WWN                     DId swName
   __________________________________________________
     1   Yes     10:00:00:05:1e:35:d5:14   2 ITSO_2005_B32
     2   No      10:00:00:05:1e:02:4e:fb   3 IBM_2005_B16


ITSO_2005_B32:admin>
```

Figure 1-233 The secPolicyShow output

For further details on configuring and implementing security and policies, please refer to *Brocade Secure Fabric Administrator's Guide*, 53-1000048-02.

1.9.9 Zoning

Zoning allows us to define specific groups of fabric-connected devices to ensure that the access between them is controlled. Be aware that devices that are not configured in a zone will not be accessible.

The Zone Admin function within WebTools is used to set up, maintain, and activate the zones across the fabric. From here we can also define aliases for members in a zone and can create the zones that form the active configuration across the fabric.

A zoning license and administrative privileges are required to access this function. All 2109 and 2005 models are delivered with the zoning license pre-installed. When administering zoning on an IBM TotalStorage SAN Switch, the following steps are recommended:

- Define zone aliases to establish groupings.
- Add zone members.
- Place zones into one or more zone configurations.
- Enable one of the zone configurations (only one can be enabled at a time).

> **Tip:** It is important to make sure that only one person is making configuration changes to your environment at any one time. Using the `killtelnet` command provides a view of who is logged in to the switch and a method for removing any sessions that should not be in place.

To access the zone administration, we click the **Zone** Admin button on the bottom left hand corner as noted in Figure 1-234.

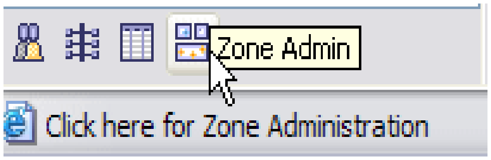
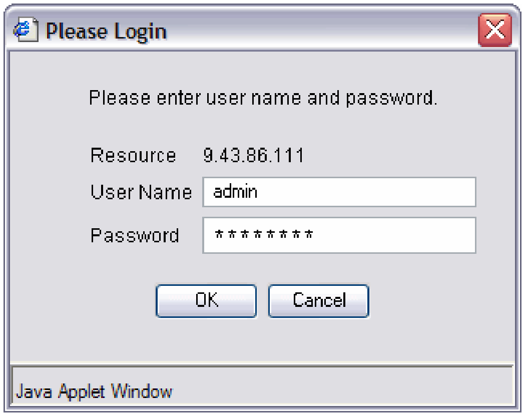


Figure 1-234 Zone Admin button

After clicking the **Zone Admin** button, we are prompted for our user name and password shown in Figure 1-235.



Please enter user name and password.

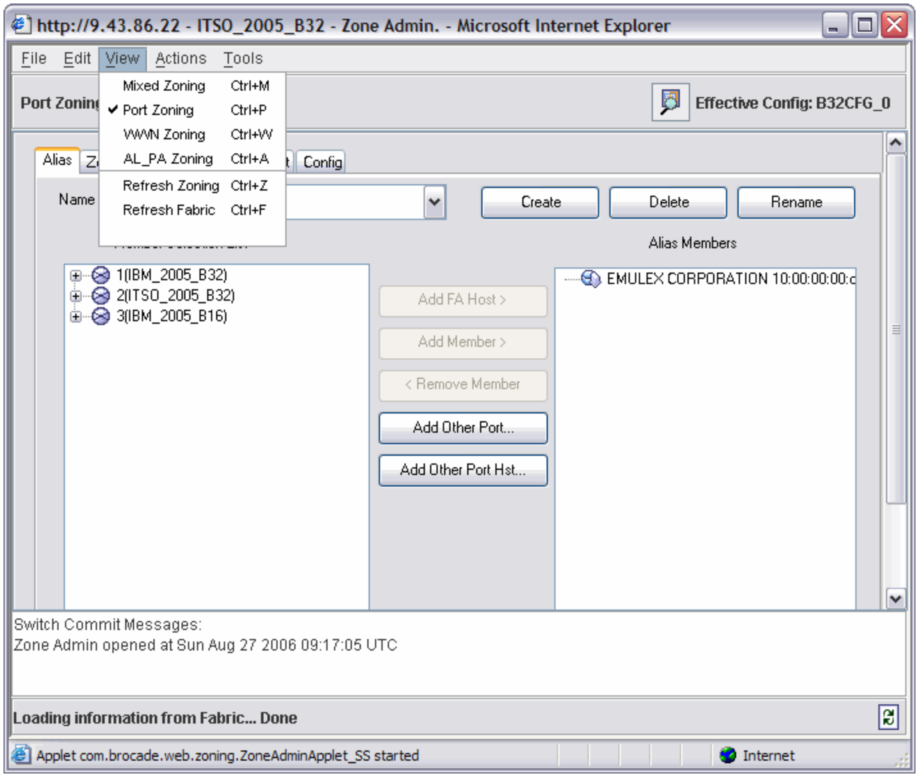
Resource 9.43.86.111

User Name admin

Password ********

Figure 1-235 Authentication

After entering user name and password, click **OK** (The defaults are *admin / password*). We can select the type of zoning we want to configure using the View drop down menu as shown in Figure 1-236. Although Mixed Zoning is the default view, our example displays the Port Zoning scheme.


http://9.43.86.22 - ITSO_2005_B32 - Zone Admin. - Microsoft Internet Explorer
File
Edit
View
Actions
Tools
Port Zoning
Mixed Zoning Ctrl+M
✓ Port Zoning Ctrl+P
WWN Zoning Ctrl+W
AL_PA Zoning Ctrl+A
Refresh Zoning Ctrl+Z
Refresh Fabric Ctrl+F
Effective Config: B32CFG_0
Alias
Config
Name
Create
Delete
Rename
Alias Members
1(IBM_2005_B32)
2(ITSO_2005_B32)
3(IBM_2005_B16)
Add FA Host >
Add Member >
< Remove Member
Add Other Port...
Add Other Port Hst...
EMULEX CORPORATION 10:00:00:00:c
Internet

Switch Commit Messages:
Zone Admin opened at Sun Aug 27 2006 09:17:05 UTC

Loading information from Fabric... Done

Applet com.brocade.web.zoning.ZoneAdminApplet_SS started

Figure 1-236 B32 Port Zoning Initial view

We describe the zoning schemes in the following sections. Using any of these methods results in our configuration being hardware enforced by the switch ASICs (hard zoned).

Mixed Zoning

In this scheme, all objects are displayed in the *Member Selection List*. Any object, being a WWN, port, AL_PA, or alias, can be selected to be managed in the *Members* list. When the Zoning management function is opened, this is the default scheme.

Working in the mixed zoning scheme allows us to define a WWN and a physical port to be within the same configuration. If we have mixed members in a zone, the zoning uses session-based hard zoning.

Port Zoning

This zoning scheme only offers physical switches and ports to be selected and defined as members for alias, zoning, QuickLoop, Fabric Assist, and configuration groups. Aliases, zones, and configuration groups which have objects other than physical ports will not be displayed in this scheme.

The main benefit of Port Zoning is that whenever a HBA to a device is replaced, for example the HBA on a server, the zoning is not affected by the change in WWN. Provided that the new device is connected to the original port, it continues to have the same access rights. However, it is extremely important to maintain port and device allocation in the fabric when using this method in order to maintain device security.

WWN Zoning

This scheme only allows aliases, zoning, and configuration file operations on WWNs, aliases, and zones. Configuration files that have objects other than WWNs are not displayed within this scheme.

The main advantage of WWN zoning is the additional security provided by tying down the access to a specific device via its unique WWN.

AL_PA Zoning

This scheme allows only aliases, zoning, and configuration file operations on AL_PAs in a QuickLoop. Any aliases, zones, and configuration files that have objects other than AL_PAs in a QuickLoop are not displayed.

1.9.10 Implementing zoning

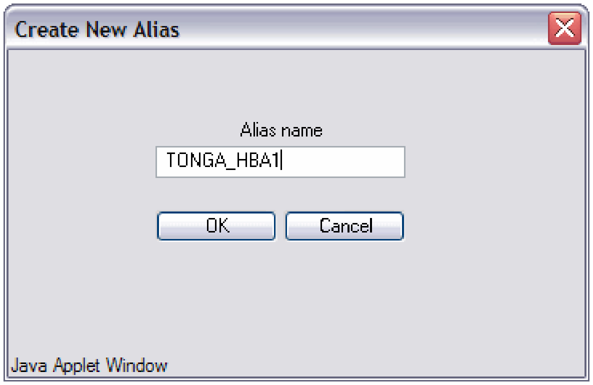
In the following examples, we show the windows in which we apply zoning concepts that have previously been discussed. For our purposes we have chosen the Mixed Zoning scheme, although the procedure is the same for Port, WWN and AL_PA schemes.

Important: Remember to back up your configuration prior to making any configuration changes. This way you can always get back to your starting point if things go awry.

Alias tab

By defining an alias to a port(s) or WWN(s), we simplify our understanding of what the device is that we are working with on the other tabs. By using a sensible naming convention, it also assists with troubleshooting at a later date by making it easier to find specific devices, especially when our SAN grows in complexity. We recommend assigning aliases and ensuring that they are maintained to correctly identify SAN components. This can be accomplished by using the **Alias** tab.

To create a new alias, we click the **Create** button and the **Create New Alias** window is displayed. Type in the new alias name and click **OK** as seen in Figure 1-237.

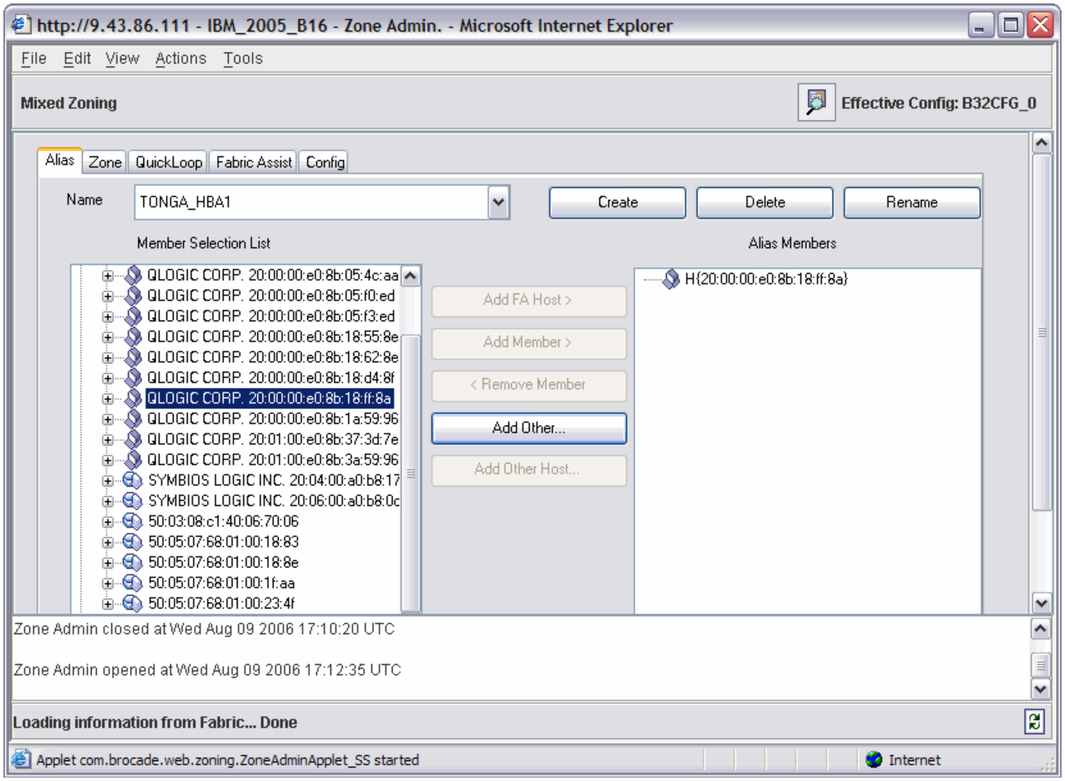


Alias name: TONGA_HBA1

Figure 1-237 B32 Create new alias

After clicking **OK**, we see the name displayed in the Name field. We can now select a member or multiple members from the *Member Selection List* on the left. We select port 4 on switch domain 1, and then click the **Add Member** button to add it to the *Alias Members List* in the right panel as shown in Figure 1-236 on page 293.

If a host or device has multiple HBAs, we might want to add more members to our alias. As we are defining an alias for one AIX® production host, we want to only define this HBA as shown. We have successfully identified the WWN of our device on switch domain 1 to have an alias of TONGA_HBA1 as shown in Figure 1-238.


File
Edit
View
Actions
Tools
Alias
Zone
QuickLoop
Fabric Assist
Config
Create
Delete
Rename
Member Selection List
Alias Members
Add FA Host >
Add Member >
< Remove Member
Add Other...
Add Other Host...
Internet

http://9.43.86.111 - IBM_2005_B16 - Zone Admin. - Microsoft Internet Explorer

Mixed Zoning

Effective Config: B32CFG_0

Name: TONGA_HBA1

Member Selection List:

QLOGIC CORP. 20:00:00:e0:8b:05:4c:aa
QLOGIC CORP. 20:00:00:e0:8b:05:f0:ed
QLOGIC CORP. 20:00:00:e0:8b:05:f3:ed
QLOGIC CORP. 20:00:00:e0:8b:18:55:8e
QLOGIC CORP. 20:00:00:e0:8b:18:62:8e
QLOGIC CORP. 20:00:00:e0:8b:18:d4:8f
QLOGIC CORP. 20:00:00:e0:8b:18:ff:8a
QLOGIC CORP. 20:00:00:e0:8b:1a:59:96
QLOGIC CORP. 20:01:00:e0:8b:37:3d:7e
QLOGIC CORP. 20:01:00:e0:8b:3a:59:96
SYMBIOS LOGIC INC. 20:04:00:a0:b8:17
SYMBIOS LOGIC INC. 20:06:00:a0:b8:0c
50:03:08:c1:40:06:70:06
50:05:07:68:01:00:18:83
50:05:07:68:01:00:18:8e
50:05:07:68:01:00:1f:aa
50:05:07:68:01:00:23:4f

Alias Members:

H{20:00:00:e0:8b:18:ff:8a}

```
Zone Admin closed at Wed Aug 09 2006 17:10:20 UTC

Zone Admin opened at Wed Aug 09 2006 17:12:35 UTC
```

Loading information from Fabric... Done

Applet com.brocade.web.zoning.ZoneAdminApplet_SS started

Figure 1-238 Alias Administration

We would follow the same procedure for all our hosts and storage before adding them to zones.

This could also be completed from the command line using the **`aliCreate`** command and use the **`aliShow`** command to display the alias as detailed in Example 1-48.

Example 1-48 Creating and viewing an alias from the command line

```
ITSO_2005_B32:admin> aliCreate “TONGA_HBA2” “20:00:00:e0:8b:18:d4:8f”
ITSO_2005_B32:admin> cfgSave
You are about to save the Defined zoning configuration. This
action will only save the changes on the Defined configuration.
Any changes made on the Effective configuration will not
take effect until it is re-enabled.
Do you want to save Defined zoning configuration only? (yes, y, no, n): [no] y

ITSO_2005_B32:admin> aliShow "TONGA*"
 alias: TONGA_HBA1
                H{20:00:00:e0:8b:18:ff:8a}
 alias: TONGA_HBA2
                H{20:00:00:e0:8b:18:d4:8f}
```

Table 1-26 describes the fields and buttons on the **Alias tab**.

Table 1-26 Alias tab description:

Button	Function
Name	Select an existing alias name to be modified.
Create	Select to create a new alias. A new alias dialog displays. Enter a new alias name that is unique. The new alias name cannot contain spaces.
Delete	Select to delete the alias selected in the Name field. Deleting an alias automatically removes it from all zones.
Rename	Select to rename the alias selected in the Name field. A dialog displays in which you can edit the alias name. Renaming an alias automatically renames it in all zones.
Member Selection List	This field contains a list of potential alias members, including switches, ports, Nodes, WWNs, and QuickLoop AL_PAs.
Add FA Host >	Use this button to add a Fabric Assist Host to the member list.
Add Member >	Select to add the item selected in the Member Selection List to the Alias Members list. You can add individual ports or an entire switch. If a switch is added, all ports on the switch are added. To add a device WWN, select either a node WWN (folder icon) or port WWN (blue circle icon) from the WWN sub-tree.
< Remove Member	Select to remove the member selected from the Alias Name Members Selection list.
Add Other Port	Select to add a switch/port combination that currently is not part of the fabric.
Add Other Port Host	Select to add a switch/port combination of a host that currently is not part of the fabric.

Selecting ports on the SAN256B

Some consideration must be taken to understand the port addressing when zoning a SAN256B. In previous versions of the Fabric OS (version 2.0 and version 3.0), the primary method for identifying a port within the fabric was the "domain, port" combination.

For example, to add port 1 on domain 5 to a zone, we would use this coding:

```
sw96:admin>zoneadd "bluezone","5,1"
```

The "domain, port" method of selecting ports cannot be used in the M48 because of the addition of slots and the high port count of the switch. This method was replaced in Fabric OS version 4.0 and onwards by two methods to specify a particular port: the slot/port method and the port area number method.

Slot/port method

To select a specific port, you must identify both the slot number and port number that you are working with.

When specifying a particular slot and port for a command, the slot number operand must be followed by the slash (/) and then a value for the port number. For example, to enable port 63, we specify:

```
   portEnable 10/15
```

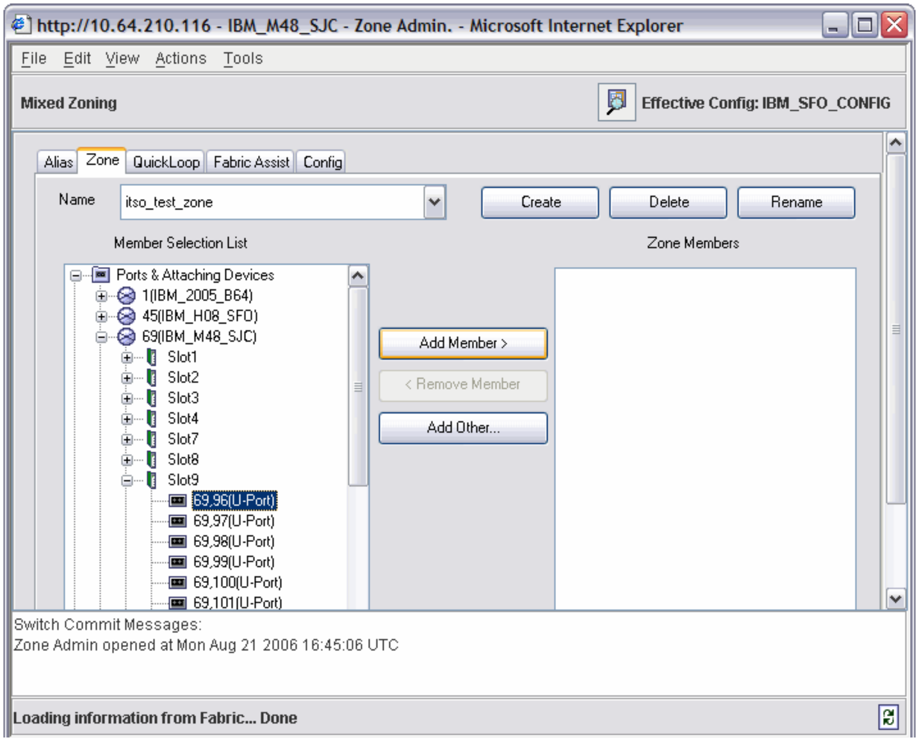
Restriction: No spaces are allowed between the slot number, the slash (/), and the port number.

Port area number method

Some commands, such as zoning commands, allow you to specify ports using the port area number method. In the Fabric OS version 4.0 and onwards, each port on a particular domain is given a unique area ID.

Use the `switchShow` command to display all ports on the current (logical) switch and their corresponding area IDs.

Figure 1-239 shows how the WebTools interface for the SAN256B Zoning view displays the slot and associated ports for a domain (switch).


http://10.64.210.116 - IBM_M48_SJC - Zone Admin. - Microsoft Internet Explorer
File Edit View Actions Tools
Mixed Zoning
Alias
Zone
QuickLoop
Fabric Assist
Config
Create
Delete
Rename
Member Selection List
Zone Members
Ports & Attaching Devices
1(IBM_2005_B64)
45(IBM_H08_SFO)
69(IBM_M48_SJC)
Slot1
Slot2
Slot3
Slot4
Slot7
Slot8
Slot9
69,96(U-Port)
69,97(U-Port)
69,98(U-Port)
69,99(U-Port)
69,100(U-Port)
69,101(U-Port)
Add Member >
< Remove Member
Add Other...

Effective Config: IBM_SFO_CONFIG

Name: itso_test_zone

Switch Commit Messages:
Zone Admin opened at Mon Aug 21 2006 16:45:06 UTC

Loading information from Fabric... Done

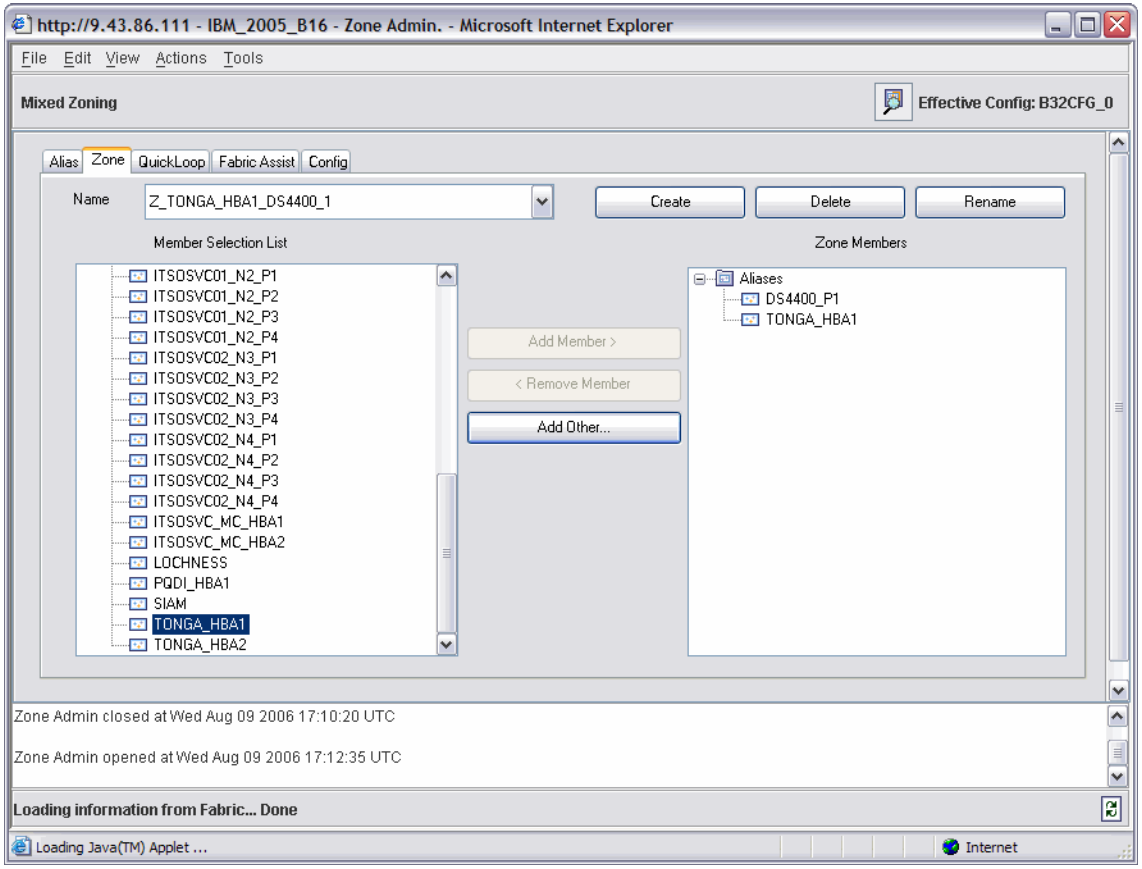
Figure 1-239 SAN256B Zoning - Slot/Port area number

Zone tab

We use the **Zone** tab to specify which switch ports are to be in the selected zone and to create and manage zones. A zone can have one or multiple members, and can include switches, ports, WWNs, aliases, AL_PAs or Quickloop. Be aware that Quickloop is no longer supported from 4.4.x FOS onwards.

> **Important:** We recommend creating individual zones of each host to the disk storage subsystems. Also, hosts should have a separate HBA for Tape communication, and again be in another individual Host / Tape zone.
>
> This small granularity of zoning removes unnecessary PLOGI activity from host to host, as well as removing the risk of problems caused by a faulty HBA affecting others.

In the example shown in Figure 1-240, we have created a zone named ***Z_TONGA_HBA1_DS4400_1***.



Name: Z_TONGA_HBA1_DS4400_1

Zone Admin closed at Wed Aug 09 2006 17:10:20 UTC

Zone Admin opened at Wed Aug 09 2006 17:12:35 UTC

Loading information from Fabric... Done

http://9.43.86.111 - IBM_2005_B16 - Zone Admin. - Microsoft Internet Explorer
File Edit View Actions Tools
Mixed Zoning
Effective Config: B32CFG_0
Alias
Zone
QuickLoop
Fabric Assist
Config
Create
Delete
Rename
Member Selection List
Zone Members
ITSOSVC01_N2_P1
ITSOSVC01_N2_P2
ITSOSVC01_N2_P3
ITSOSVC01_N2_P4
ITSOSVC02_N3_P1
ITSOSVC02_N3_P2
ITSOSVC02_N3_P3
ITSOSVC02_N3_P4
ITSOSVC02_N4_P1
ITSOSVC02_N4_P2
ITSOSVC02_N4_P3
ITSOSVC02_N4_P4
ITSOSVC_MC_HBA1
ITSOSVC_MC_HBA2
LOCHNESS
PQDI_HBA1
SIAM
TONGA_HBA1
TONGA_HBA2
Add Member >
< Remove Member
Add Other...
Aliases
DS4400_P1
TONGA_HBA1
Loading Java(TM) Applet ...
Internet

Figure 1-240 SAN32B Creating a Zone

First we click the **Create** button. Then we add the new zone name in the pop-up window and click **OK**. We then select our previously created aliases, *TONGA_HBA1* and *DS4400_1* and select the **Add Member** button.

As mentioned in the previous recommendation, we could add another HBA installed in server to this zone, but we do not recommend adding other hosts. We choose to define a separate zone for each host. In our example the host is not configured to allow multiple paths to the same device; as such, we do not add the second path in for the DS4400 disk array. In a more resilient setup, we would have both the host HBA as well as two connections to the storage.

Table 1-27 describes the fields and buttons on the **Zone** tab.

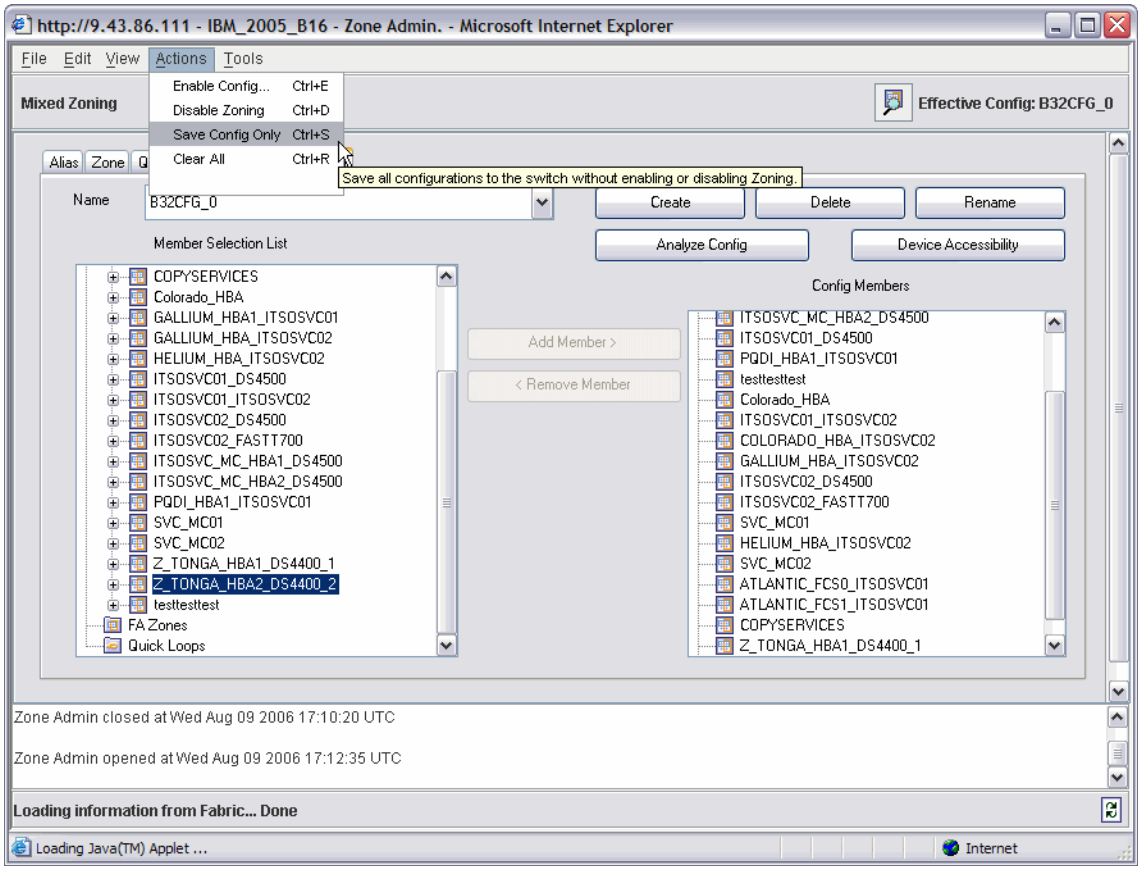
Table 1-27 Zone tab description

Button	**Function**
Name	Select an existing alias name to be modified.
Create	Select to create a new alias. A new alias dialog displays. Enter a new alias name that is unique. The new alias name cannot contain spaces.
Delete	Select to delete the alias selected in the Name field. Deleting an alias automatically removes it from all zones.
Rename	Select to rename the alias selected in the Name field. A dialog displays in which you can edit the alias name. Renaming an alias automatically renames it in all zones.
Member Selection List	This field contains a list of potential alias members, including switches, ports, Nodes, WWNs, and QuickLoop AL_PAs.
Add Member >	Select to add the item selected in the Member Selection List to the Alias Members list. You can add individual ports or an entire switch. If a switch is added, all ports on the switch are added. To add a device WWN, select either a node WWN (folder icon) or port WWN (blue circle icon) from the WWN sub-tree.
< Remove Member	Select to remove the member selected from the Alias Name Members Selection list.
Add Other Port	Select to add a switch/port combination that currently is not part of the fabric.

Config tab

We now use the **Config** tab to create/update a zone configuration. Zone configurations are used to enable or disable a group of zones at the same time. In this example we already have an active configuration on the switch and as such we use the **Add Member >** button to move our newly created zones, listed in the left column, to the Config Members list on the right.

This process creates a configuration containing all the desired zones we want to activate. We then save the configuration by selecting the **Save Config Only** option from the *Actions* pulldown menu. This only saves the configuration to nonvolatile storage, it does not bring the configuration active and is detailed in Figure 1-241.


http://9.43.86.111 - IBM_2005_B16 - Zone Admin. - Microsoft Internet Explorer
File Edit View Actions Tools
Enable Config... Ctrl+E
Disable Zoning Ctrl+D
Save Config Only Ctrl+S
Clear All Ctrl+R
Mixed Zoning
Effective Config: B32CFG_0
Alias Zone Q
Name
Create Delete Rename
Analyze Config Device Accessibility
Member Selection List
Config Members
Add Member >
< Remove Member
COPYSERVICES
Colorado_HBA
GALLIUM_HBA1_ITSOSVC01
GALLIUM_HBA_ITSOSVC02
HELIUM_HBA_ITSOSVC02
ITSOSVC01_DS4500
ITSOSVC01_ITSOSVC02
ITSOSVC02_DS4500
ITSOSVC02_FASTT700
ITSOSVC_MC_HBA1_DS4500
ITSOSVC_MC_HBA2_DS4500
PQDI_HBA1_ITSOSVC01
SVC_MC01
SVC_MC02
Z_TONGA_HBA1_DS4400_1
Z_TONGA_HBA2_DS4400_2
testtesttest
FA Zones
Quick Loops
ITSOSVC_MC_HBA2_DS4500
ITSOSVC01_DS4500
PQDI_HBA1_ITSOSVC01
testtesttest
Colorado_HBA
ITSOSVC01_ITSOSVC02
COLORADO_HBA_ITSOSVC02
GALLIUM_HBA_ITSOSVC02
ITSOSVC02_DS4500
ITSOSVC02_FASTT700
SVC_MC01
HELIUM_HBA_ITSOSVC02
SVC_MC02
ATLANTIC_FCS0_ITSOSVC01
ATLANTIC_FCS1_ITSOSVC01
COPYSERVICES
Z_TONGA_HBA1_DS4400_1
Loading Java(TM) Applet ...
Internet

Name: B32CFG_0

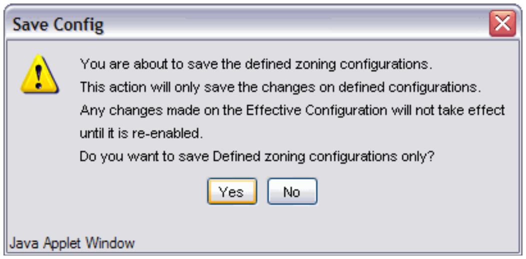
Save all configurations to the switch without enabling or disabling Zoning.

```
Zone Admin closed at Wed Aug 09 2006 17:10:20 UTC

Zone Admin opened at Wed Aug 09 2006 17:12:35 UTC
```

Loading information from Fabric... Done

Figure 1-241 SAN32B Save config only

At this stage we are just saving this example as advised by the pop-up window in Figure 1-242.


Save Config
Yes
No
Java Applet Window

You are about to save the defined zoning configurations.
This action will only save the changes on defined configurations.
Any changes made on the Effective Configuration will not take effect until it is re-enabled.
Do you want to save Defined zoning configurations only?

Figure 1-242 Zoning save config popup window

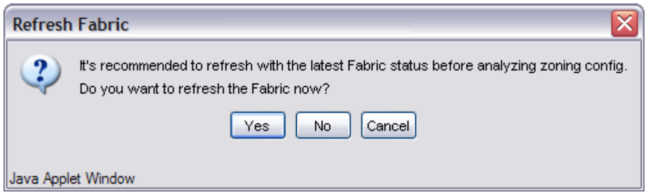
Table 1-28 contains a description of the fields and buttons on the **Config** tab.

Table 1-28 Config tab description

Button	**Function**
Name	Select an existing configuration to modify.
Create	Click to create a new configuration. A dialog displays. Enter the name of the new configuration. All names must be unique and contain no spaces.
Delete	Click to delete the configuration selected in the Cfg Name field.
Rename	Click to edit the name of the configuration selected in the Cfg Name field.
Member Selection List	This field provides a list of the zones and QuickLoops available to add to the configuration.
Add Member >	Click to add the switch selected in the Zone/QLoop Selection List to the Config Members list.
< Remove Member	Click to remove the selected member from the Config Members list.
Analyze Config	Analyzes the configuration that is selected along with its member zones and aliases. A zoning configuration error window appears in the event of a conflict.
Device Accessibility	View initiator/target accessibility matrix based on selected configuration.

After our configuration is saved, we click the **Analyze Config** button as shown in Figure 1-241 on page 302. This checks the validity of our zoning configuration, and alerts us to ports and WWNs that we have not included.

We are prompted to refresh the current configuration from the switch as shown here in Figure 1-243. The Analyze operation checks the most recent information from the switch.

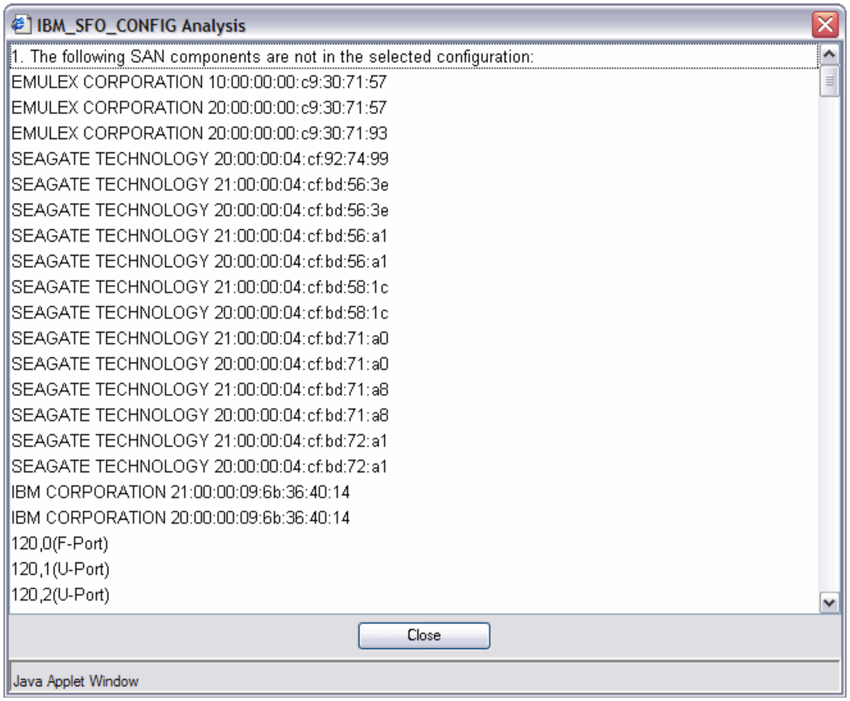


Refresh Fabric

It's recommended to refresh with the latest Fabric status before analyzing zoning config.
Do you want to refresh the Fabric now?

Figure 1-243 Refresh Fabric prompt

Remember to review the Analyze output and make adjustments (if appropriate) before activating the configuration. An example of the Analyze output is given in Figure 1-244.



```
1. The following SAN components are not in the selected configuration:
EMULEX CORPORATION 10:00:00:00:c9:30:71:57
EMULEX CORPORATION 20:00:00:00:c9:30:71:57
EMULEX CORPORATION 20:00:00:00:c9:30:71:93
SEAGATE TECHNOLOGY 20:00:00:04:cf:92:74:99
SEAGATE TECHNOLOGY 21:00:00:04:cf:bd:56:3e
SEAGATE TECHNOLOGY 20:00:00:04:cf:bd:56:3e
SEAGATE TECHNOLOGY 21:00:00:04:cf:bd:56:a1
SEAGATE TECHNOLOGY 20:00:00:04:cf:bd:56:a1
SEAGATE TECHNOLOGY 21:00:00:04:cf:bd:58:1c
SEAGATE TECHNOLOGY 20:00:00:04:cf:bd:58:1c
SEAGATE TECHNOLOGY 21:00:00:04:cf:bd:71:a0
SEAGATE TECHNOLOGY 20:00:00:04:cf:bd:71:a0
SEAGATE TECHNOLOGY 21:00:00:04:cf:bd:71:a8
SEAGATE TECHNOLOGY 20:00:00:04:cf:bd:71:a8
SEAGATE TECHNOLOGY 21:00:00:04:cf:bd:72:a1
SEAGATE TECHNOLOGY 20:00:00:04:cf:bd:72:a1
IBM CORPORATION 21:00:00:09:6b:36:40:14
IBM CORPORATION 20:00:00:09:6b:36:40:14
120,0(F-Port)
120,1(U-Port)
120,2(U-Port)
```

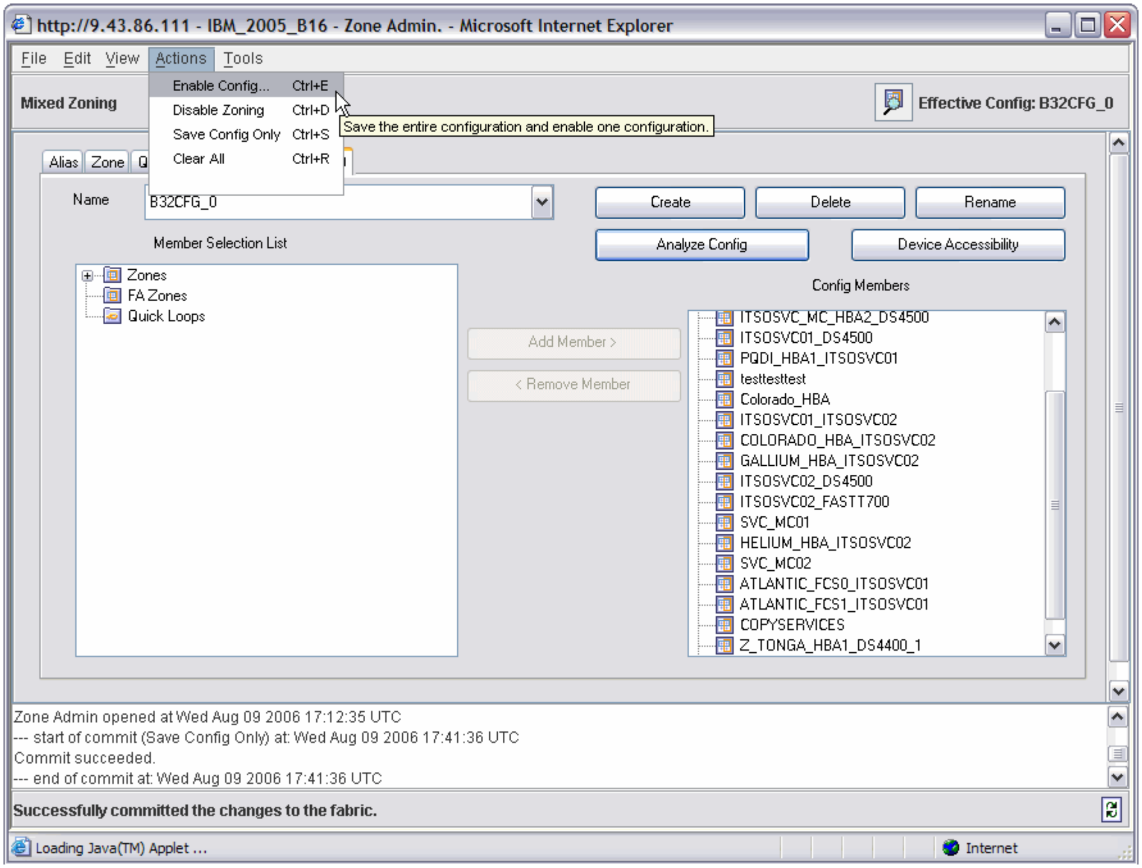
Figure 1-244 Sample of Analyze Config output

The Zoning Configuration Analyze window displays a summary of the saved configuration and attempts to point out some of the zoning conflicts before applying the changes to the switch. Some of the potential errors it might catch are:

- Ports/WWNs/Devices that are part of the selected configuration, but not part of the fabric
- Zones with only a single member

Activating a zoning configuration

To make the zoning definitions active, we have to enable the configuration that we have built. We do this by using the **Enable Config...** selection from the *Actions* pulldown menu shown in Figure 1-245.

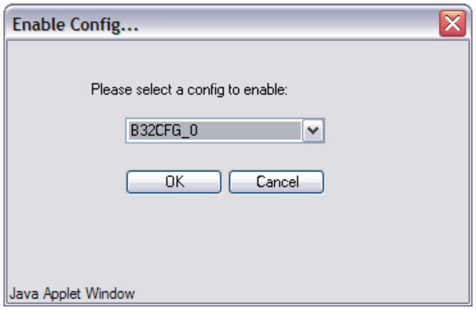

http://9.43.86.111 - IBM_2005_B16 - Zone Admin. - Microsoft Internet Explorer
File Edit View Actions Tools
Enable Config... Ctrl+E
Disable Zoning Ctrl+D
Save Config Only Ctrl+S
Clear All Ctrl+R
Save the entire configuration and enable one configuration.
Mixed Zoning
Effective Config: B32CFG_0
Alias Zone Q
Name B32CFG_0
Create
Delete
Rename
Analyze Config
Device Accessibility
Member Selection List
Zones
FA Zones
Quick Loops
Add Member >
< Remove Member
Config Members
ITSOSVC_MC_HBA2_DS4500
ITSOSVC01_DS4500
PQDI_HBA1_ITSOSVC01
testtesttest
Colorado_HBA
ITSOSVC01_ITSOSVC02
COLORADO_HBA_ITSOSVC02
GALLIUM_HBA_ITSOSVC02
ITSOSVC02_DS4500
ITSOSVC02_FASTT700
SVC_MC01
HELIUM_HBA_ITSOSVC02
SVC_MC02
ATLANTIC_FCS0_ITSOSVC01
ATLANTIC_FCS1_ITSOSVC01
COPYSERVICES
Z_TONGA_HBA1_DS4400_1
Loading Java(TM) Applet ...
Internet

```
Zone Admin opened at Wed Aug 09 2006 17:12:35 UTC
--- start of commit (Save Config Only) at: Wed Aug 09 2006 17:41:36 UTC
Commit succeeded.
--- end of commit at: Wed Aug 09 2006 17:41:36 UTC
```

Successfully committed the changes to the fabric.

Figure 1-245 SAN32B enabling the config using Web Tools

We are prompted to select which configuration we would like to enable, as shown in Figure 1-246.


Enable Config...

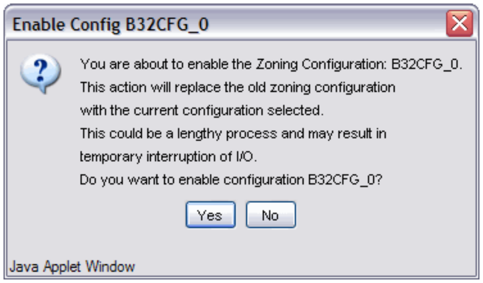
Please select a config to enable:

B32CFG_0

Figure 1-246 SAN32B zoning prompt

Then we are prompted, as shown in Figure 1-247, to confirm that we want to enable the configuration.

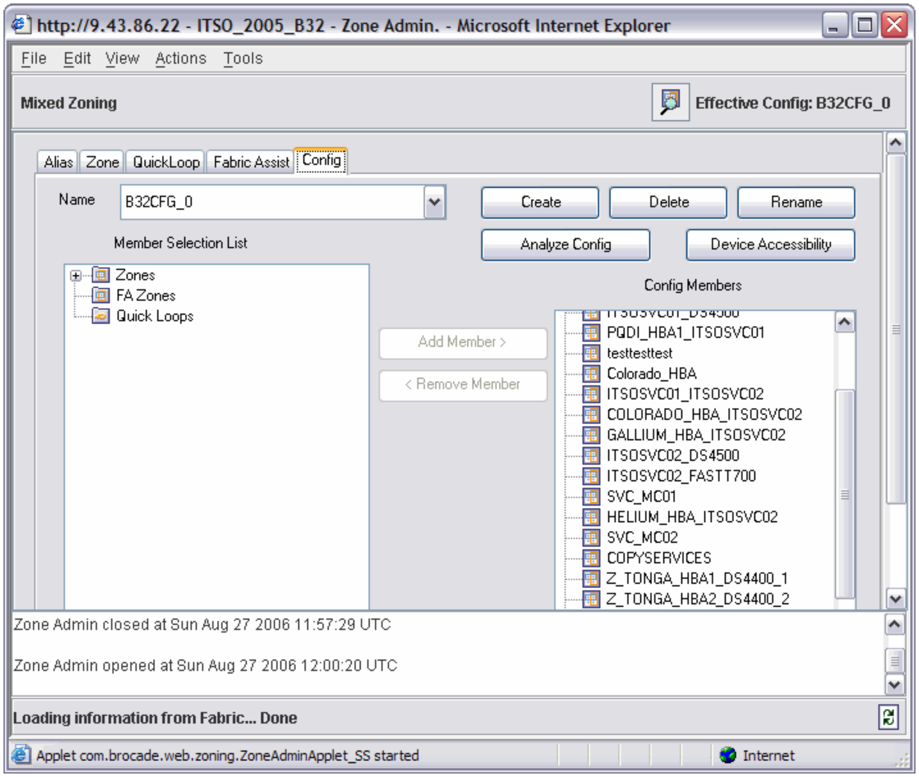
> **Attention:** Take care when enabling zone configurations. Adding new zones does not impact any currently running definitions, although removing a zone might have a large impact to the current environment.


Enable Config B32CFG_0

You are about to enable the Zoning Configuration: B32CFG_0.
This action will replace the old zoning configuration
with the current configuration selected.
This could be a lengthy process and may result in
temporary interruption of I/O.
Do you want to enable configuration B32CFG_0?

Figure 1-247 SAN32B Config Enable warning

At this point the new zone configuration definitions take place on the SAN fabric. Messages appear in the `syslogd` area of the window to show successful completion. The window is also updated to reflect the enabled configuration as shown in Figure 1-248.


http://9.43.86.22 - ITSO_2005_B32 - Zone Admin. - Microsoft Internet Explorer
File Edit View Actions Tools
Mixed Zoning
Alias Zone QuickLoop Fabric Assist Config
Create
Delete
Rename
Analyze Config
Device Accessibility
Member Selection List
Zones
FA Zones
Quick Loops
Add Member >
< Remove Member
Config Members
Internet

Effective Config: B32CFG_0

Name: B32CFG_0

Config Members: ITSOSVC01_DS4500, PQDI_HBA1_ITSOSVC01, testtesttest, Colorado_HBA, ITSOSVC01_ITSOSVC02, COLORADO_HBA_ITSOSVC02, GALLIUM_HBA_ITSOSVC02, ITSOSVC02_DS4500, ITSOSVC02_FASTT700, SVC_MC01, HELIUM_HBA_ITSOSVC02, SVC_MC02, COPYSERVICES, Z_TONGA_HBA1_DS4400_1, Z_TONGA_HBA2_DS4400_2

```
Zone Admin closed at Sun Aug 27 2006 11:57:29 UTC

Zone Admin opened at Sun Aug 27 2006 12:00:20 UTC
```

Loading information from Fabric... Done

Applet com.brocade.web.zoning.ZoneAdminApplet_SS started

Figure 1-248 SAN32B Enable zoning configuration, successfully completed

Again we can complete the zoning using either the GUI or CLI. First we create the zone using **`zoneCreate`**, then we save the zone configuration using **`cfgSave`**. After this is done, we can then check our zoning configuration using the zoneShow command. As before, we then have to add our zone to the configuration file; this time we use the **`cfgAdd`** command. Finally we use **`cfgEnable`** to enable the new zoning configuration. Each of these stages is presented in Example 1-49.

We can check the active configuration at any point in time using the **`cfgActvShow`** command.

Example 1-49 Zoning configuration

```
ITSO_2005_B32:admin> zoneCreate “Z_TONGA_HBA2_DS4400_2”, “DS4400_P2”,
“TONGA_HBA2”
ITSO_2005_B32:admin> cfgSave
You are about to save the Defined zoning configuration. This
action will only save the changes on the Defined configuration.
```

```
Any changes made on the Effective configuration will not
take effect until it is re-enabled.
Do you want to save Defined zoning configuration only? (yes, y, no, n): [no] y

ITSO_2005_B32:admin> zoneShow Z_TONGA*
 zone:  Z_TONGA_HBA1_DS4400_1
                DS4400_P1; TONGA_HBA1
 zone:  Z_TONGA_HBA2_DS4400_2
                DS4400_P2; TONGA_HBA2
 zone:  Z_TONGA_TAPE
                TAPE_LIB; TONGA_HBA1
 zone:  Z_TONGA_TAPE2
                TONGA_HBA2; TAPE_LIB_DRIVE2

ITSO_2005_B32:admin>cfgAdd “B32_CFG_0”, “Z_TONGA_HBA1_DS4400_1”,
“Z_TONGA_HBA2_DS4400_2”, “Z_TONGA_TAPE”,”Z_TONGA_TAPE2”
ITSO_2005_B32:admin> cfgSave
ITSO_2005_B32:admin> cfgEnable “B32_CFG_0”
You are about to enable a new zoning configuration.
This action will replace the old zoning configuration with the current
configuration selected.
Do you want to enable 'B32_CFG_0' configuration  (yes, y, no, n): [no] y
zone config "B32_CFG_0" is in effect
Updating flash ...
```

Modifying an existing configuration

When adding a new host or a new device into the fabric, changes to the zoning are necessary. For example, we add a new host, define a *newhost* alias, create a *newhost_DS4400* zone. Using the procedures previously described in this topic, we then add the *newhost_DS4400* zone to our configuration.

We then have two choices, immediate implementation, or we can save our updates and perform the activate at a later time:

- Choose **Enable Config...** from the *Actions* pulldown menu, the changes are saved and take effect immediately.
- Choose **Save Config only** from the *Actions* pulldown menu. The changes are saved, but does not take effect immediately. For the changes to take effect, we have to select the configuration in the names list, and then select **Enable Config...** from the *Actions* pulldown menu.

Zoning and E_Ports

When creating a zone, we only work with device ports or host ports (F_Ports, FL_Ports, L_Ports). Any ISL Ports (E_Ports) should not be included in zone definitions.

Consider the example presented in Figure 1-249.

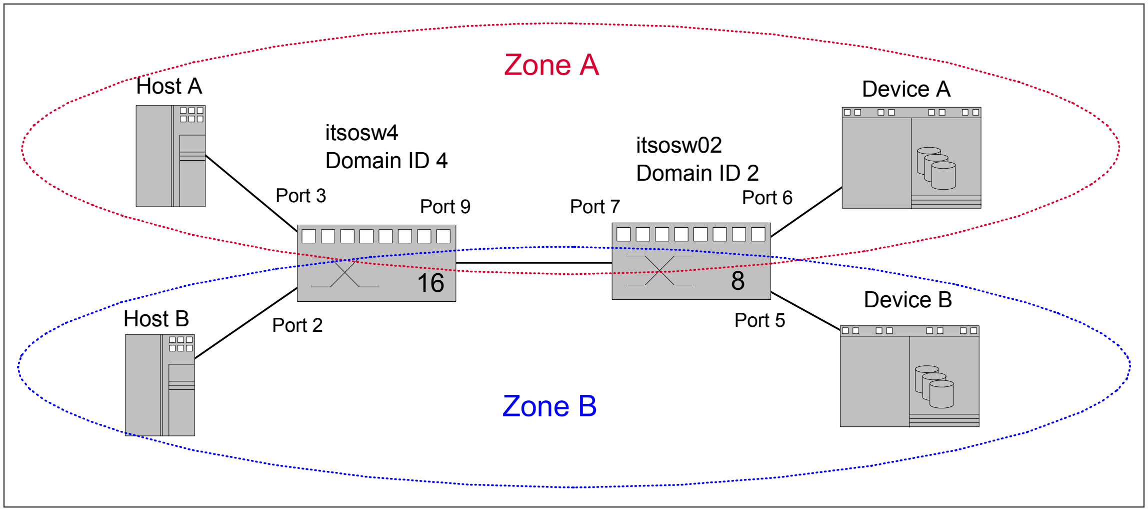

Zone A
Host A
Device A
itsosw4
Domain ID 4
itsosw02
Domain ID 2
Port 3
Port 9
Port 7
Port 6
16
8
Host B
Port 2
Port 5
Device B
Zone B

Figure 1-249 Zoning implementation — E_Ports and Zoning

To create Zone A, we include:

- Domain ID 4, Port 3 (4,3)
- Domain ID 2, Port 6 (2,6)

But we *do not* include any ISL ports, that is to say:

- Domain ID 4, Port 9 (4,9)
- Domain ID 2, Port 7 (2,7)

Similarly, to create Zone B, we only include:

- Domain ID 4, Port 2 (4,2)
- Domain ID 2, Port 5 (2,5)

Zones do not affect data traffic across ISLs in cascaded switch configurations. Because Hard Zoning enforcement is performed at the destination, an ISL can carry data traffic from all zones.

Therefore, when dealing with zoning, the fabric should be seen as a “cloud” to which are attached devices and hosts. That is, we define the end-to-end destinations, and do not include the path to get there.

1.9.11 Multiple switch environments

In the topics that follow we describe multiple switch environment considerations.

InterSwitch Links

There are three features available on the IBM TotalStorage SAN Switch that allow for remote distribution of the fabric:

- ISL R_RDY mode
- Remote switch
- Extended fabrics

We discuss these features in the topics that follow.

ISL R_RDY Mode

ISL R_RDY Mode was introduced in v3.1 of FOS. It replaces the Remote Switch feature, is more flexible and is supported by many gateway manufacturers. It is used to configure a link between switches that passes through a gateway.

When first establishing a connection to another switch or Node, switch ports initialize using Exchange Link Parameters (ELP) mode 1. Gateways however, expect an initialization that uses ELP mode 2. Setting a port ISL R_RDY mode prepares the port for Gateway connections by causing the port initialization to use the expected method (ELP mode 2). Therefore, the WAN gateway does not have to support a special mode for these switches.

To enable R_RDY on port 9, we use the **`portcfgislmode`** command as seen in Example 1-50:

Example 1-50 Enable ISL R_RDY mode using portcfgislmode

```
IBM_2005_B16:admin> portcfgislmode 9, 1
Committing configuration...done.
ISL R_RDY Mode is enabled for port 9. Please make sure the PID
formats are consistent across the entire fabric.
IBM_2005_B16:admin>
```

After ensuring that the above steps have been performed on the other remote switch, and all parameters, including core PID, match — our remote switch link is now operational.

> **Note:** We do not discuss Remote Switch functionality within this book, because ISL R_RDY mode has replaced it.

Trunking

Now we describe the Trunking feature.

ISL Trunking is an optionally licensed product on the b-type family of switches. It requires a separate *Performance Monitor* License key to be purchased and installed.

The ISL Trunking feature allows up to four Interswitch Links (ISLs) to merge logically into a single link. An ISL is a connection between two switches through an Expansion Port (E_Port).

When using ISL Trunking to aggregate bandwidth of up to four or eight ports (depending upon the switch model) the speed of the ISLs between switches in a fabric is correspondingly multiplied by up to 4 or 8. For example, at 4 Gbps speeds, trunking on a SAN-16B switch which is capable of 4 port trunking delivers ISL throughput of 8, 12, and up to 16 Gbps.

As such, with Extended ISL Trunking and 4 Gbps port speed we can now double the number of ISLs and we can have a total capacity in a single trunk of 32 Gbps on the switch models that support 8 port trunks. See Table 1-5 on page 12 for details on the supported ISL trunking across the current b-type switch family.

ISL Trunking can be managed using Telnet commands or the WebTools interface.

Advantages of ISL Trunking

The ISL Trunking feature has many advantages; ISL Trunking supports high-bandwidth, large-scale SANs which include core switches. The primary task of ISL Trunking is to provide high bandwidth path between switches in a fabric, while balancing the traffic across the individual links and maintaining In-Order Delivery of data packets to their destination.

Attention: In-Order Delivery is the recommended setting in an IBM fabric, this setting can be changed by the user.

ISL Trunking uses frame-level load balancing, as opposed to Fibre Channel Shortest Path First (FSPF), to achieve faster fabric convergence, as well as higher availability of the fabric. See Table 1-5 on page 11 for information regarding the throughput improvements that can be seen when implementing trunking.

Trunking groups, ports, and masters

ISL Trunking dynamically performs load balancing, at the frame level, across a set of available links between two adjacent switches to establish a trunking group. Ports that belong to a trunking group are called trunking ports. One port is used to assign traffic for the group, and is referred to as the trunking master.

Trunking groups

A trunking group is identified by the trunking master that represents the entire group. The rest of the group members are referred to as slave links that help the trunking master direct traffic across ISLs, allowing efficient and balanced in-order communication.

Trunking ports

Trunking ports in a trunking group should meet the following criteria:

- Port must be configured as E_Ports.
- Ports must reside in the same contiguous four-port groups in a 2 Gb environment and 8-port groups in a 4 Gb environment. Each switch has the four port quads identified on the port panel with alternating colors:
  - Group 1: port 0 to port 3
  - Group 2: port 4 to port 7
  - Group 3: port 8 to port 11
  - Group 4:port 12 to port 15
  - and so on...
- Trunking Ports must run at the same speed, 2 Gbps or 4 Gbps speeds.
- Each switch must have a trunking license installed.
- The cable difference between all ports in a trunking group must be less than 500 meters.

Trunking masters

The trunking master implicitly defines the trunking group. All ports with the same master are considered to be part of the same group. Each trunking group includes a single trunking master and several trunking slave links. The first ISL found in any trunking group is assigned to be the trunking master, also known as the principal ISL. After the trunking group is fully established, all data packets intended for transmission across the trunk are dynamically distributed at frame level across the ISLs in the trunking group, while preserving in-order delivery.

Installing ISL Trunking

The b-type family of switches require that a *Performance Monitor* license be installed to enable trunking using either Telnet or the Web interface.

Both switches at either end of an ISL Trunk require an active license for trunking to work. A license might have been installed in the switch at the factory. If not, contact your switch supplier to obtain a license key.

Administering ISL Trunking

The ISL Trunking feature is managed by performing some administration tasks. These tasks include:

- Enabling or disabling the trunking
- Enabling and disabling ports of a switch
- Setting the speed of a port
- Debugging a trunking link failure

The ISL Trunking feature is administered using Telnet commands.

ISL Trunking Telnet commands

Table 1-29 describes the Telnet commands used to manage the ISL Trunking feature.

Table 1-29 ISL Telnet commands

Command	**Description**	**Example**

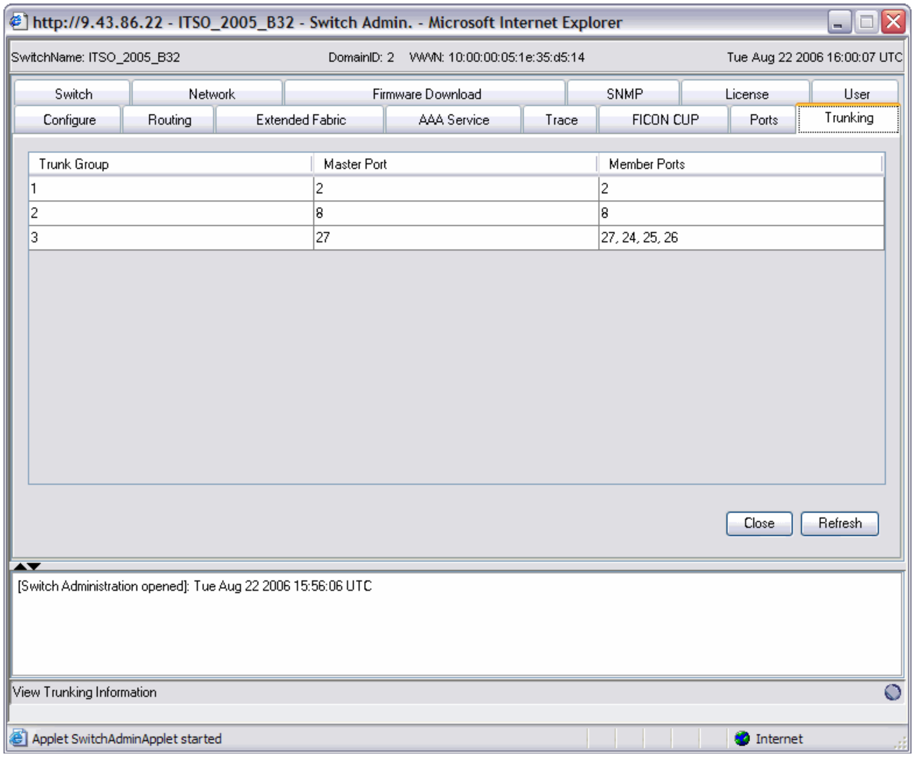
`portCfgTrunkport`	Use this command to configure a port to be enabled or disabled for trunking.	To enable port 5 for ISL TRUNKING, enter:
		`portCfgTrunkport 5, 1`
		To disable port 5 for ISL TRUNKING, enter:
		`portCfgTrunkport 5, 0`

`switchCfgTrunk`	Use this command to enable or disable trunking on all ports of a switch.	To enable trunking on all ports of a switch, enter:
		`switchCfgTrunk 1`
		To disable ISL Trunking on all ports of a switch, enter:
		`switchCfgTrunk 0`

`trunkDebug`	Use this command to debug a trunk link failure.	To debug ports 1 and 2, enter: `trunkDebug 1, 2`
`trunkshow`	Use this command to display ISL Trunking membership information.	To display ISL Trunking membership information about users, enter: `trunkshow`

Trunking within WebTools

This panel is used for viewing the trunking configuration only, as seen in Figure 1-250.


http://9.43.86.22 - ITSO_2005_B32 - Switch Admin. - Microsoft Internet Explorer
Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Ports
Trunking
Close
Refresh
Internet

SwitchName: ITSO_2005_B32 DomainID: 2 WWN: 10:00:00:05:1e:35:d5:14 Tue Aug 22 2006 16:00:07 UTC

Trunk Group	Master Port	Member Ports
1	2	2
2	8	8
3	27	27, 24, 25, 26

[Switch Administration opened]: Tue Aug 22 2006 15:56:06 UTC

View Trunking Information

Applet SwitchAdminApplet started

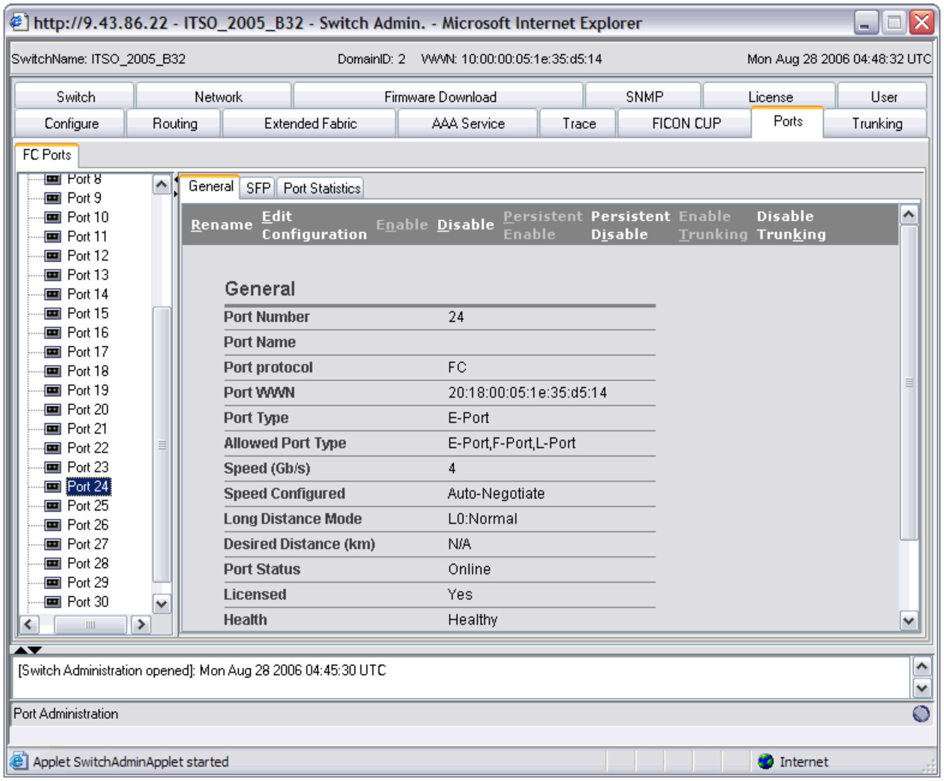
Figure 1-250 Web Tools Trunking tab

After you unlock the ISL Trunking license, you must re-initialize the ports being used for ISLs so that they recognize that trunking is enabled. This procedure only has to be performed once.

To re-initialize the ports, you can either disable and then re-enable the switch using the **`switchDisable`** then **`switchEnable`** commands, or disable and then re-enable the affected ports using **`portDisable`** ***`[slot/]port`*** and **`portEnable`** ***`[slot/]port`***. By disabling and re-enabling the switch itself, all ports are available for trunking.

Alternatively we can select the individual ports from the Web Tools admin interface and enable ISL trunking from there.

Disabling or enabling trunking is done through the Port Setting panel. This is shown in Figure 1-251 from ports 8-16 by checking the **Enable Trunking** box.


http://9.43.86.22 - ITSO_2005_B32 - Switch Admin. - Microsoft Internet Explorer
Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Ports
Trunking
FC Ports
Port 8
Port 9
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15
Port 16
Port 17
Port 18
Port 19
Port 20
Port 21
Port 22
Port 23
Port 24
Port 25
Port 26
Port 27
Port 28
Port 29
Port 30
General
SFP
Port Statistics
Rename
Edit Configuration
Enable
Disable
Persistent Enable
Persistent Disable
Enable Trunking
Disable Trunking
Port Administration
Applet SwitchAdminApplet started
Internet

SwitchName: ITSO_2005_B32 DomainID: 2 WWN: 10:00:00:05:1e:35:d5:14 Mon Aug 28 2006 04:48:32 UTC

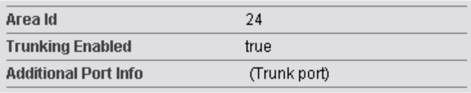
General

Port Number	24
Port Name	
Port protocol	FC
Port WWN	20:18:00:05:1e:35:d5:14
Port Type	E-Port
Allowed Port Type	E-Port,F-Port,L-Port
Speed (Gb/s)	4
Speed Configured	Auto-Negotiate
Long Distance Mode	L0:Normal
Desired Distance (km)	N/A
Port Status	Online
Licensed	Yes
Health	Healthy

[Switch Administration opened]: Mon Aug 28 2006 04:45:30 UTC

Figure 1-251 Enable trunking on port

Figure 1-252 shows the additional items displayed in the Ports tab window, when we scroll the window. As you can see we have trunking enabled on port 24 and it is currently configured as a trunk port.



Area Id	24
Trunking Enabled	true
Additional Port Info	(Trunk port)

Figure 1-252 Web Tools Port tab additional details

Long Distance

Extended Fabrics can increase the allowable distance between two switches and is an optionally licensed product that runs from Fabric OS version v4.0 and onwards.

The Extended Fabrics feature creates an interconnected fabric at distances of up to 100 km using 1, 2 or 4 Gbps speed and L2 distance mode. However with the introduction of LD distance mode we can now support 250 km at 2 Gbps and 500 km at 1Gbps.

Extended Fabrics optimizes the internal buffering algorithm for IBM TotalStorage SAN Switches. It provides maximum buffering between E_Ports that are connected over an extended distance through buffer re-configuration. This results in line speed performance of close to full Fibre Channel speed for switches that are interconnected at up to 500 km, thus providing the highest possible performance for transfers between switches.

The Fibre Channel connection extensions can be provided by extended distance SFPs, Fibre Channel repeaters, or wave division multiplexing (WDM) devices.

Note: Performance can vary depending on the condition of the fiber optic connections between the switches. Losses due to splicing, connectors, tight bends, and other degradation can affect the performance over the link and the maximum distance possible.

As previously discussed, to enable Extended Fabrics, an Extended Fabrics license must be installed.

Note: To enable Extended Fabrics in a fabric created with 2005 switches, each switch in the fabric must be configured individually.

Using Extended Fabrics

We can configure ports to support long distance links through the Telnet or WebTools interfaces.

For fabrics that contain a combination of b-type models, the `fabric.ops.mode.longDistance` parameter must be set to 0 (the default). We also have to ensure that the ports on both ends of the ISL have the same configuration and that the SFPs used are qualified.

Configuring Extended Fabrics

There are six possible long distance levels for a port and these are shown in Table 1-30. Ports are grouped into 8-port blocks, each of which share a common pool of frame buffers.

Certain buffers are dedicated for each port, and others are shared among the ports. In Extended Fabric mode, one port is given an increase of dedicated buffers from this pool.

The total number of frame buffers in a quad is limited, and the Extended Fabric port matrix introduces a combination of long distance ports that are available. This is shown in Table 1-30.

Table 1-30 Extended ISL Modes

Mode	Buffer Allocation			Distance	Distance	Distance	Oldest	License
	1Gb/s	2Gb/s	4Gb/s	@1Gb/s	@2Gb/s	@4Gb/s	FOS	Req'd
L0	5(26)	5(26)	5(26)	10 km	5 km	2 km	All	No
LE	11	16	26	10km	10 km	10 km	v3,v4	No
L0.5	18	31	56	25 km	25 km	25 km	3.1,4.1,5	Yes
L1	31	56	106	50 km	50 km	50 km	All	Yes
L2	56	106	206	100 km	100 km	100 km	All	Yes
LD	Auto	Auto	Auto	Auto (Max 500km)	Auto (Max250 km)	Auto (Max 100km)	3.1,4.1,5 (depends on model)	Yes
LS	varies	varies	varies	varies (Max 500km)	varies (Max 250km)	varies (Max 100km)	v5.1.0	Yes

Where the buffer allocation and distance vary, these are based upon user specified distances.

For dynamic long distance links, you can approximate the number of buffer credits using the following formula:

Buffer credits = [(distance in km) * (data rate) * 1000] / 2112

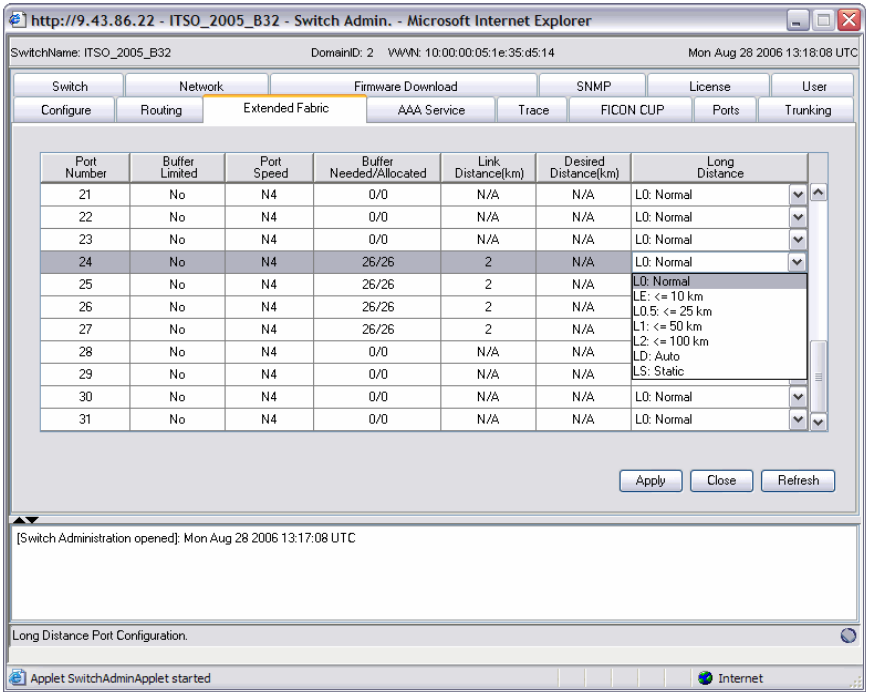
The data rate is 1.0625 for 1 Gbps, 2.125 for 2 Gbps, and 4.25 for 4 Gbps, and Fibre Channel. This formula provides the minimum number of credits that are allocated to a given port; the actual number is likely higher.

Setting the port configuration

We can configure a port to support long distance links by using the Telnet command **`portCfgLongDistance`** or by using the WebTools.

Extended Fabrics within WebTools

The **Extended Fabric** tab within WebTools allows us to configure long distance ports. The SAN256B has slot subtabs when configuring a given port as shown in Figure 1-253. With a SAN256B, first we select the slot tab, then highlight port 0. For all other models we would just highlight the given port we want to configure as long distance.


http://9.43.86.22 - ITSO_2005_B32 - Switch Admin. - Microsoft Internet Explorer
Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Ports
Trunking
L0: Normal
LE: <= 10 km
L0.5: <= 25 km
L1: <= 50 km
L2: <= 100 km
LD: Auto
LS: Static
Apply
Close
Refresh
Internet

SwitchName: ITSO_2005_B32 DomainID: 2 WWN: 10:00:00:05:1e:35:d5:14 Mon Aug 28 2006 13:18:08 UTC

Port Number	Buffer Limited	Port Speed	Buffer Needed/Allocated	Link Distance(km)	Desired Distance(km)	Long Distance
21	No	N4	0/0	N/A	N/A	L0: Normal
22	No	N4	0/0	N/A	N/A	L0: Normal
23	No	N4	0/0	N/A	N/A	L0: Normal
24	No	N4	26/26	2	N/A	L0: Normal
25	No	N4	26/26	2	N/A	
26	No	N4	26/26	2	N/A	
27	No	N4	26/26	2	N/A	
28	No	N4	0/0	N/A	N/A	
29	No	N4	0/0	N/A	N/A	
30	No	N4	0/0	N/A	N/A	L0: Normal
31	No	N4	0/0	N/A	N/A	L0: Normal

[Switch Administration opened]: Mon Aug 28 2006 13:17:08 UTC

Long Distance Port Configuration.

Applet SwitchAdminApplet started

Figure 1-253 B32 Extended Fabric tab

After highlighting the port to configure, we go to the **Long Distance** column on the far right hand side and click the down arrow to show the options available for configuration.

Table 1-31 lists the details with the **Extended Fabric** tab.

Table 1-31 Extended Fabric configuration

Port Number	Port Number for all switch models, see Slot Number tab description for M48 model number
Buffer Limited	If large distances are set onto various ports within an 8-port block, the remaining ports within that block might have to have their allocated buffer count reduced to enable the long distance configuration.
Port Speed	1G, 2G, 4G as set speeds N1, N2 N4 as negotiated speeds
Buffer Needed/Allocated	Actual buffer usage of port
Link Distance	Real distance in kilometers
Desired Distance	Desired distance in kilometers for the port based on port speed
Long Distance	L0 = Normal value, long distance disabled LE = Extended normal enabled **The following items require Extended Fabric License:** **L0.5** = 25 km or less **L1** = Medium long distance enabled, 50 km or less **L2** = Long distance enabled, 100 km or less **LD** = Dynamic link enabled, operates at distances up to 500 km for 1Gb/s, 250 km for 2Gb/s, or 125 km for 4Gb/s depending upon frame buffer availability within the port group **LS** = Static setting enabled. Buffer credits statically configured based on link distance, operates at distances up to 500 km for 1Gb/s, 250 km for 2Gb/s, or 125 km for 4Gb/s depending upon frame buffer availability within the port group
Slot Number tab	Subtab for the slots in the M12 and M14 displaying the ports on the given slot for the logical switch
Apply	Apply and commit changes to the switch
Close	Close Administrator Window
Refresh	Refresh the view with current data from switch

Merging

Merging a SAN fabric occurs where two or more separate fabrics are combined. An example of this is shown in Figure 1-254.

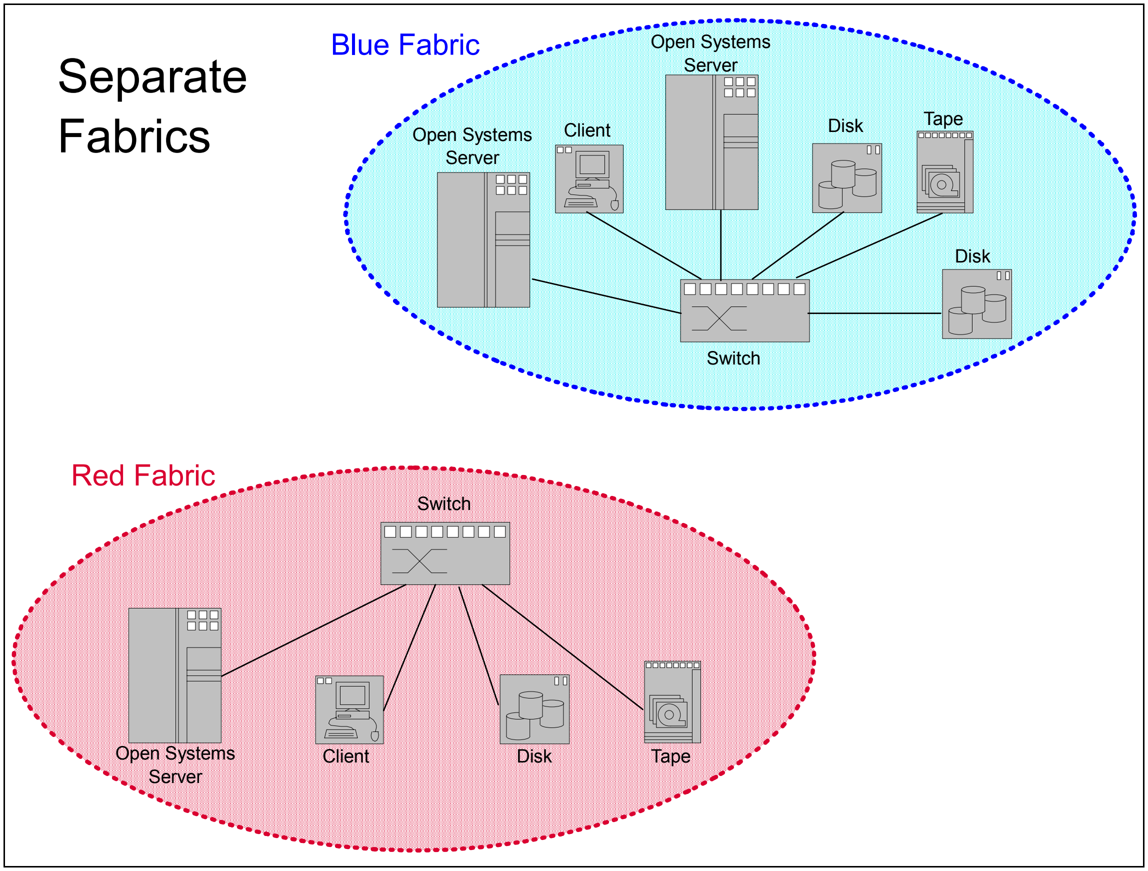

Separate Fabrics
Blue Fabric
Open Systems Server
Open Systems Server
Client
Disk
Tape
Disk
Switch
Red Fabric
Switch
Open Systems Server
Client
Disk
Tape

Figure 1-254 Two separate SAN fabrics

These separate SAN fabrics can be merged to form a larger SAN fabric by connecting the switches using an Inter-Switch Link (ISL) as shown in Figure 1-255.

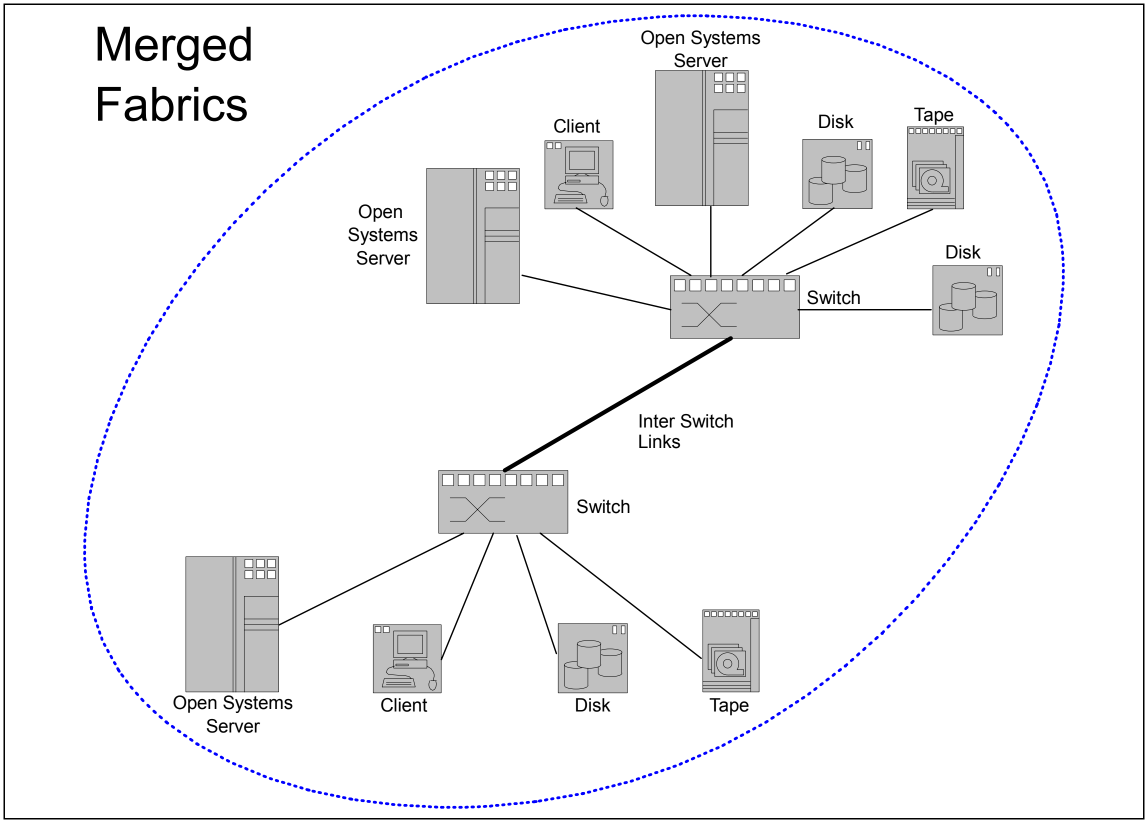

Merged Fabrics
Open Systems Server
Client
Disk
Tape
Open Systems Server
Disk
Switch
Inter Switch Links
Switch
Open Systems Server
Client
Disk
Tape

Figure 1-255 A merged fabric

The zoning information for each fabric is retained as are the domain IDs for the switches, assuming that there are no conflicting definitions.

This could happen when an organization acquires another company or when two business units within one company merge. The result is that a SAN fabric is extended through the addition of another complete fabric.

Important: You should always disable a switch before adding it to an existing fabric.

Some conflicts might occur as two fabrics are merged. Some of the most common sources of conflict are:

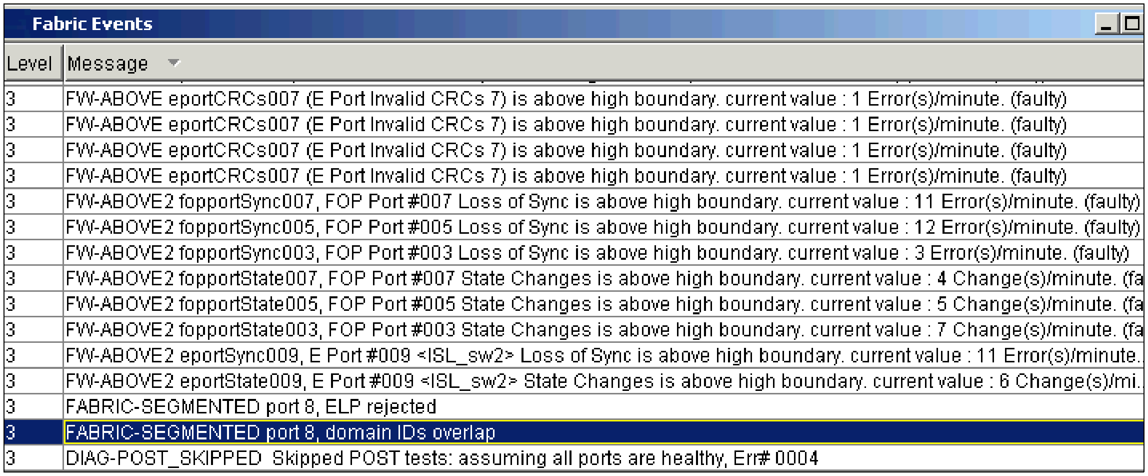
- Duplicate domain ID
- Zoning configuration conflicts
- Operating parameters inconsistency (for example, Core PID format)

When this occurs, part of the SAN fabric is said to be *segmented*. You can identify a segmentation from the slow flashing orange LED on the ISL port.

The following section describes these three conflicts and their possible solution.

Duplicate domain IDs

Domain IDs are used to uniquely identify a switch within a fabric. Therefore, each switch within the same fabric must have a unique domain ID. Duplicate domains causes the ISL between the two switches to be segmented as shown in Figure 1-256.



Level	Message
3	FW-ABOVE eportCRCs007 (E Port Invalid CRCs 7) is above high boundary. current value : 1 Error(s)/minute. (faulty)
3	FW-ABOVE eportCRCs007 (E Port Invalid CRCs 7) is above high boundary. current value : 1 Error(s)/minute. (faulty)
3	FW-ABOVE eportCRCs007 (E Port Invalid CRCs 7) is above high boundary. current value : 1 Error(s)/minute. (faulty)
3	FW-ABOVE eportCRCs007 (E Port Invalid CRCs 7) is above high boundary. current value : 1 Error(s)/minute. (faulty)
3	FW-ABOVE2 fopportSync007, FOP Port #007 Loss of Sync is above high boundary. current value : 11 Error(s)/minute. (faulty)
3	FW-ABOVE2 fopportSync005, FOP Port #005 Loss of Sync is above high boundary. current value : 12 Error(s)/minute. (faulty)
3	FW-ABOVE2 fopportSync003, FOP Port #003 Loss of Sync is above high boundary. current value : 3 Error(s)/minute. (faulty)
3	FW-ABOVE2 fopportState007, FOP Port #007 State Changes is above high boundary. current value : 4 Change(s)/minute. (fa
3	FW-ABOVE2 fopportState005, FOP Port #005 State Changes is above high boundary. current value : 5 Change(s)/minute. (fa
3	FW-ABOVE2 fopportState003, FOP Port #003 State Changes is above high boundary. current value : 7 Change(s)/minute. (fa
3	FW-ABOVE2 eportSync009, E Port #009 <ISL_sw2> Loss of Sync is above high boundary. current value : 11 Error(s)/minute.
3	FW-ABOVE2 eportState009, E Port #009 <ISL_sw2> State Changes is above high boundary. current value : 6 Change(s)/mi.
3	FABRIC-SEGMENTED port 8, ELP rejected
3	FABRIC-SEGMENTED port 8, domain IDs overlap
3	DIAG-POST_SKIPPED Skipped POST tests: assuming all ports are healthy, Err# 0004

Figure 1-256   Domain ID segmentation error log

To solve this overlap, change the domain ID of one of the switches participating in the ISL. This can be done using the WebTools GUI in the **Switch Settings** tab or using the **`configure`** telnet command as shown in 1.7.3, “Connecting to the switch” on page 52.

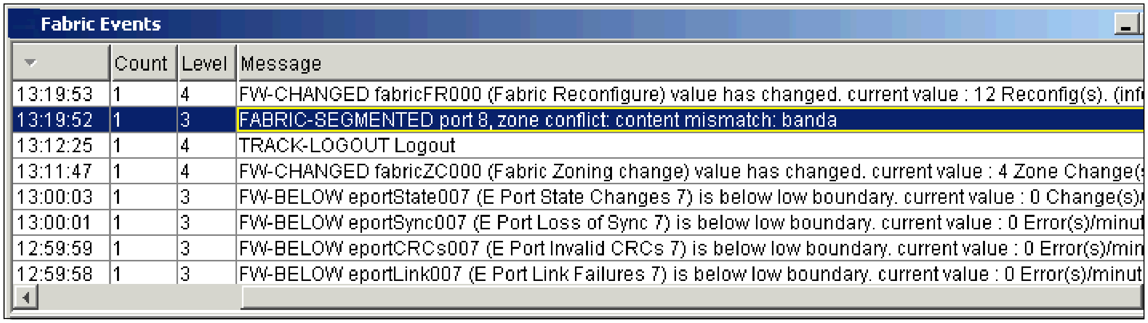
Domain ID overlap can be easily avoided by disabling the switches first using the `switchDisable` command. When bringing back the switches online automatically, the domain ID is negotiated and set to a valid value.

Zoning configuration conflicts

When merging two fabrics, zoning information from the two previously separate fabrics is merged as much as possible into the new fabric.

Sometimes, zoning inconsistency can occur and zoning information cannot be merged.

An example of segmentation due to zoning is shown in Figure 1-257.



	Count	Level	Message
13:19:53	1	4	FW-CHANGED fabricFR000 (Fabric Reconfigure) value has changed. current value : 12 Reconfig(s). (inf
13:19:52	1	3	FABRIC-SEGMENTED port 8, zone conflict: content mismatch: banda
13:12:25	1	4	TRACK-LOGOUT Logout
13:11:47	1	4	FW-CHANGED fabricZC000 (Fabric Zoning change) value has changed. current value : 4 Zone Change(
13:00:03	1	3	FW-BELOW eportState007 (E Port State Changes 7) is below low boundary. current value : 0 Change(s)/
13:00:01	1	3	FW-BELOW eportSync007 (E Port Loss of Sync 7) is below low boundary. current value : 0 Error(s)/minut
12:59:59	1	3	FW-BELOW eportCRCs007 (E Port Invalid CRCs 7) is below low boundary. current value : 0 Error(s)/min
12:59:58	1	3	FW-BELOW eportLink007 (E Port Link Failures 7) is below low boundary. current value : 0 Error(s)/minut

Figure 1-257 Zone conflict error log

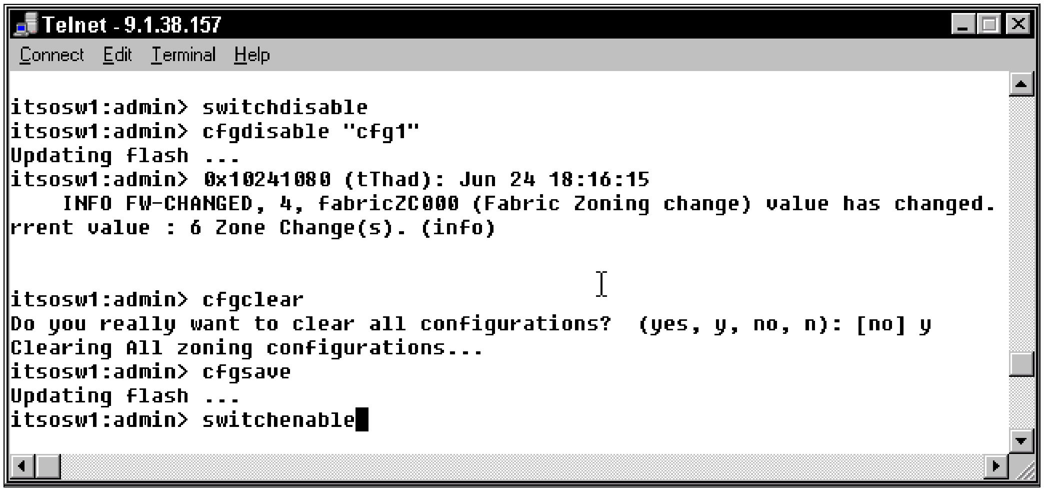
In the example above, we have a different active configuration enabled on each of the two fabrics, and each of the configurations we have an alias defined for *banda*, each alias definition pointing to a different switch/port.

One of the solutions is to make sure, before attempting the merge, that zoning information on both fabrics does not have any duplicate name definitions.

The other solution is to make sure that the switch we are adding to the fabric is cleared of any zoning information. This can be done by following this process:

1. Issue the **`switchdisable`** command to disable the switch.
2. Disable the active configuration using **`cfgdisable`**.
3. Issue the **`cfgclear`** command to clear all zoning information.
4. Issue the **`cfgsave`** command to save the changes.
5. Issue the **`switchenable`** command to enable the switch.

Figure 1-258 shows an example command flow of this process.



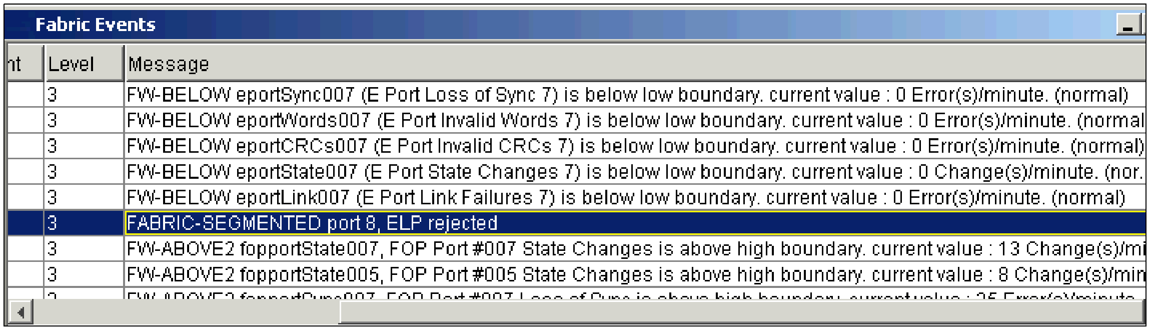
```
itsosw1:admin> switchdisable
itsosw1:admin> cfgdisable "cfg1"
Updating flash ...
itsosw1:admin> 0x10241080 (tThad): Jun 24 18:16:15
    INFO FW-CHANGED, 4, fabricZC000 (Fabric Zoning change) value has changed.
rrent value : 6 Zone Change(s). (info)


itsosw1:admin> cfgclear
Do you really want to clear all configurations?  (yes, y, no, n): [no] y
Clearing All zoning configurations...
itsosw1:admin> cfgsave
Updating flash ...
itsosw1:admin> switchenable
```

Figure 1-258   Clearing all zoning information

Operating parameters conflicts

Conflicts due to fabric wide operating parameters are less common since default values for these settings suit most requirements. They can occur when dealing with multi vendor environment or distance solution installations, for example.

Error log messages vary a lot depending on the source of the problem. An example is shown in Figure 1-259.



nt	Level	Message
	3	FW-BELOW eportSync007 (E Port Loss of Sync 7) is below low boundary. current value : 0 Error(s)/minute. (normal)
	3	FW-BELOW eportWords007 (E Port Invalid Words 7) is below low boundary. current value : 0 Error(s)/minute. (normal
	3	FW-BELOW eportCRCs007 (E Port Invalid CRCs 7) is below low boundary. current value : 0 Error(s)/minute. (normal)
	3	FW-BELOW eportState007 (E Port State Changes 7) is below low boundary. current value : 0 Change(s)/minute. (nor.
	3	FW-BELOW eportLink007 (E Port Link Failures 7) is below low boundary. current value : 0 Error(s)/minute. (normal)
	3	FABRIC-SEGMENTED port 8, ELP rejected
	3	FW-ABOVE2 fopportState007, FOP Port #007 State Changes is above high boundary. current value : 13 Change(s)/mi
	3	FW-ABOVE2 fopportState005, FOP Port #005 State Changes is above high boundary. current value : 8 Change(s)/min

Figure 1-259   Fabric parameter segmentation error log

In the example above, we have core PID set to **`on`** in one fabric and not in the other which caused the segmentation.

One solution to this problem is to make sure the fabric wide operating parameters are consistent across all participating switches.

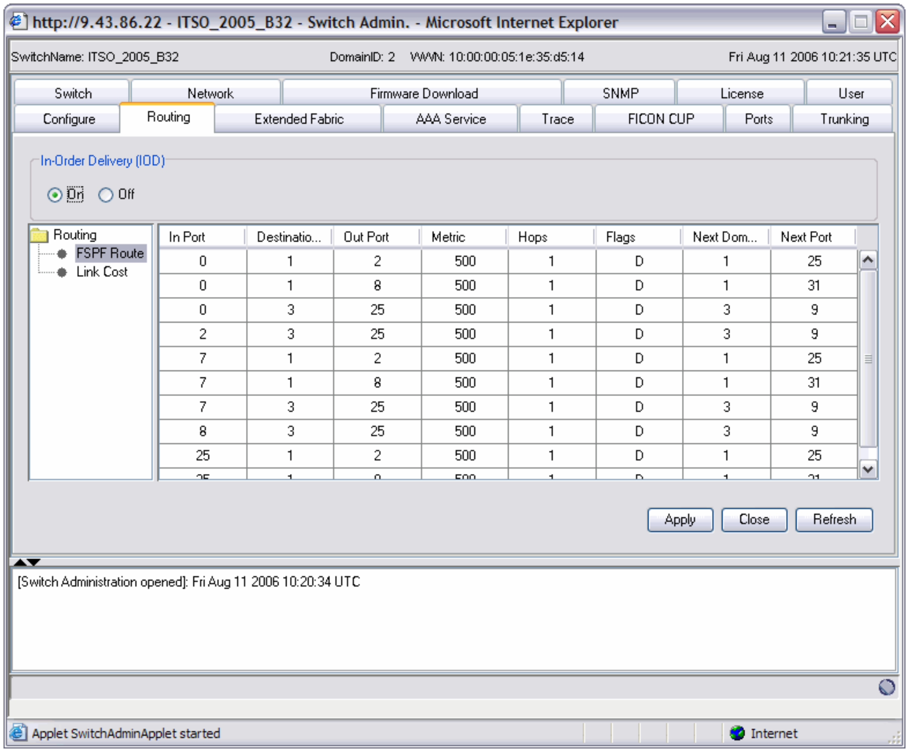
If default values are used, then follow these steps to reset the settings:

1. Telnet into the switch that you are adding, for example, **`telnet 9.1.38.1.157`**, and press Enter.
2. Login, enter the switch userid and password.
3. Disable the switch with **`switchdisable`**
4. Reset parameters using **`configdefault`**
5. Set IBM fabric parameters **`iodset`** used to force in order frame delivery) and **`dlsreset`** (used to enable dynamic sharing).
6. Use **`configure`** to set required domain ID and other specific parameters, ensuring all except the domain ID are identical.
7. Reboot the switch using the **`reboot`** or **`fastboot`** commands (the switch is enabled after the boot completes).

The reboot at the end of this procedure is required because some system parameters are cached and as such the reboot helps to prevent inconsistencies.

Routing

In Figure 1-260, we show the **Routing tab** with the default exchange based routing policy enabled. When a device-based or port-based routing policy is enabled, the interface is different: as we also see the Dynamic Load Sharing radio buttons displayed.


http://9.43.86.22 - ITSO_2005_B32 - Switch Admin. - Microsoft Internet Explorer
Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Ports
Trunking
Routing
FSPF Route
Link Cost
Apply
Close
Refresh
Internet

SwitchName: ITSO_2005_B32 DomainID: 2 WWN: 10:00:00:05:1e:35:d5:14 Fri Aug 11 2006 10:21:35 UTC

In-Order Delivery (IOD)

● On ○ Off

In Port	Destinatio...	Out Port	Metric	Hops	Flags	Next Dom...	Next Port
0	1	2	500	1	D	1	25
0	1	8	500	1	D	1	31
0	3	25	500	1	D	3	9
2	3	25	500	1	D	3	9
7	1	2	500	1	D	1	25
7	1	8	500	1	D	1	31
7	3	25	500	1	D	3	9
8	3	25	500	1	D	3	9
25	1	2	500	1	D	1	25

[Switch Administration opened]: Fri Aug 11 2006 10:20:34 UTC

Applet SwitchAdminApplet started

Figure 1-260 Routing tab

Dynamic Load Sharing (DLS)

Routing is generally based on the incoming port and the destination domain. This means that all the traffic coming in from a port (either E_Port or Fx_Port) directed to the same remote domain is routed through the same output E_Port.

To optimize fabric routing, when there are multiple equivalent paths to a remote switch, traffic is shared among all the paths. Load sharing is recomputed when a switch is booted up or every time a change in the fabric occurs. A change in the fabric is defined as an E_Port going up or down, or an Fx_Port going up or down.

In an IBM fabric, if DLS is turned off, load sharing is performed only at boot time or when an Fx_Port comes up. Optimal load sharing is rarely achieved with DLS disabled.

If DLS is turned on, routing changes can affect working ports. For example, if an Fx_Port goes down, another Fx_Port can be rerouted from one E_Port to a different E_Port. The switch minimizes the number of routing changes, but some are necessary in order to achieve optimal load sharing.

Turning on DLS can affect performance when using it in conjunction with the In-Order Delivery option.

In-Order Delivery (IOD)

Use the IOD option to enforce in-order delivery of frames during a fabric topology change. In a stable fabric, frames are always delivered in-order, even when the traffic between switches is shared among multiple paths. However, when topology changes occur in the fabric (for instance, a link goes down), traffic is rerouted around the failure. When topology changes occur, generally, some frames are delivered out-of-order. This option ensures that frames are not delivered out-of-order, even during fabric topology changes.

In an IBM fabric, the IOD option is to be set on.

This option should be used with care, because it can cause a delay in the establishment of a new path when a topology change occurs. This command should only be used if there are devices connected to the fabric that do not tolerate occasional out-of-order delivery of frames.

FSPF Route

As shown in Figure 1-260 on page 326, the FSPF Route option is selected (highlighted) under the *Routing* tree. The main area of the window then displays the FSPF routing table, including the destination domain and port, hop count, and the metric being the cost assigned to that link. We define the different columns in Table 1-32.

Table 1-32 FSPF Route field descriptions

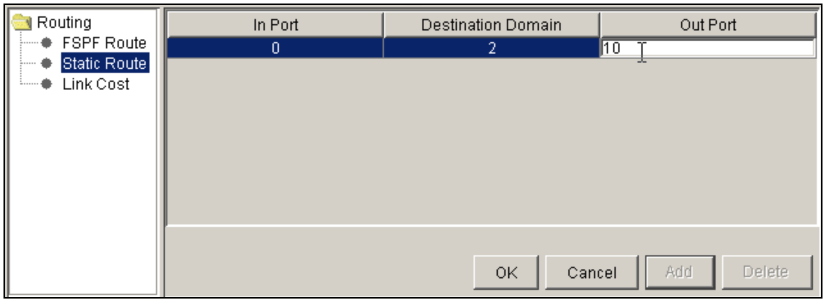
Field	**Description**
In Port	Displays the Port number where the frames enter the switch.
Destination Domain	Displays the destination domain ID for the participating static routes for a particular In Port. The destination domain is the target of the out port.
Out Port	Displays the Out port. It should be within the range of ports that are available for static routes for the current domain. More than one out port can be used for any In port with a different domain id. Each domain id requires an out port.
Metric	Displays the calculated cost of reaching the destination domain.
Hops	Displays the number of hops in the “shortest path” route.
Flags	Displays whether the route is Static (*S*) or Dynamic (*D*).
Next Domain	Displays the next domain ID in the routing path. The Next Domain is the switch that the “Out Port” is connected to.

Field	Description
Next Port	Displays the next Port in the routing path. The Next Port is the port number that the “Out Port” is physically connected to.

Static Route

This section can be used to define static routes. A static route is a route that is defining a specific path, and does not change when a topology change occurs, unless the path defined by the route becomes unavailable. Be aware that in order to define a static route, port-based routing must be active.

In Figure 1-261 we are defining a static route so that all frames received on port *0* with a destination domain of *2* are transmitted through port *10*. Clicking **OK** adds our definition to the list. We then have to click **Apply** to bring this definition active; the active definition can be seen in the FSPF routing table in Table 1-32 on page 327 identified by the *S* flag. To remove a static route, we have to select the specific definition in the static routes list and then click **Delete**.

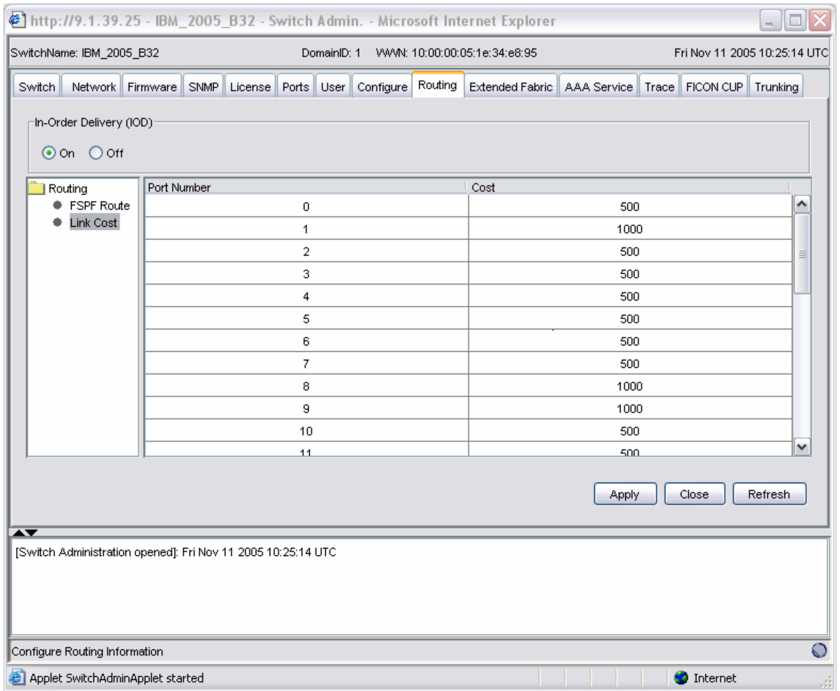


In Port	Destination Domain	Out Port
0	2	10

Figure 1-261 Routing - Static Route

Link cost

By selecting the next option under the *Routing* tree, we can view the link cost for a specific link as shown in Figure 1-262. By double-clicking in the *Cost* field for the specific port, we are able to modify the cost. This setting has an effect on the cost value the local switch has for this link. It uses this value to calculate the lowest cost path to a destination on other switch(es) within the fabric. For a 1 Gbps per second ISL, the default cost is 1000. For a 2 Gbps ISL, the default cost is 500. Valid values for link cost are from 1 to 9999.


http://9.1.39.25 - IBM_2005_B32 - Switch Admin. - Microsoft Internet Explorer
Switch
Network
Firmware
SNMP
License
Ports
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Trunking
Routing
FSPF Route
Link Cost
Apply
Close
Refresh

SwitchName: IBM_2005_B32 DomainID: 1 WWN: 10:00:00:05:1e:34:e8:95 Fri Nov 11 2005 10:25:14 UTC

In-Order Delivery (IOD)

● On ○ Off

Port Number	Cost
0	500
1	1000
2	500
3	500
4	500
5	500
6	500
7	500
8	1000
9	1000
10	500
11	500

[Switch Administration opened]: Fri Nov 11 2005 10:25:14 UTC

Configure Routing Information

Applet SwitchAdminApplet started

Internet

Figure 1-262 Routing link cost

1.9.12 FCIP/iFCP

The FCIP protocol is supported within the b-type family of products, by the SAN-16B-R, SAN18B-R and the new FR4-18i routing blade for the SAN256B. An FCIP license is required to use this functionality. These are discussed in detail within the Redbooks publication, *SAN Multiprotocol Routing: An Introduction and Implementation*, SG24-7321.

1.10 Health and troubleshooting

In the topics that follow we overview the steps that can be taken to ascertain the health of the SAN fabric, and troubleshoot problems.

1.10.1 SAN Health

SAN Health is a very powerful tool that helps a SAN administrator or SAN user optimize the existing SAN. The tool allows you to collect data and analyze this data for potential issues.

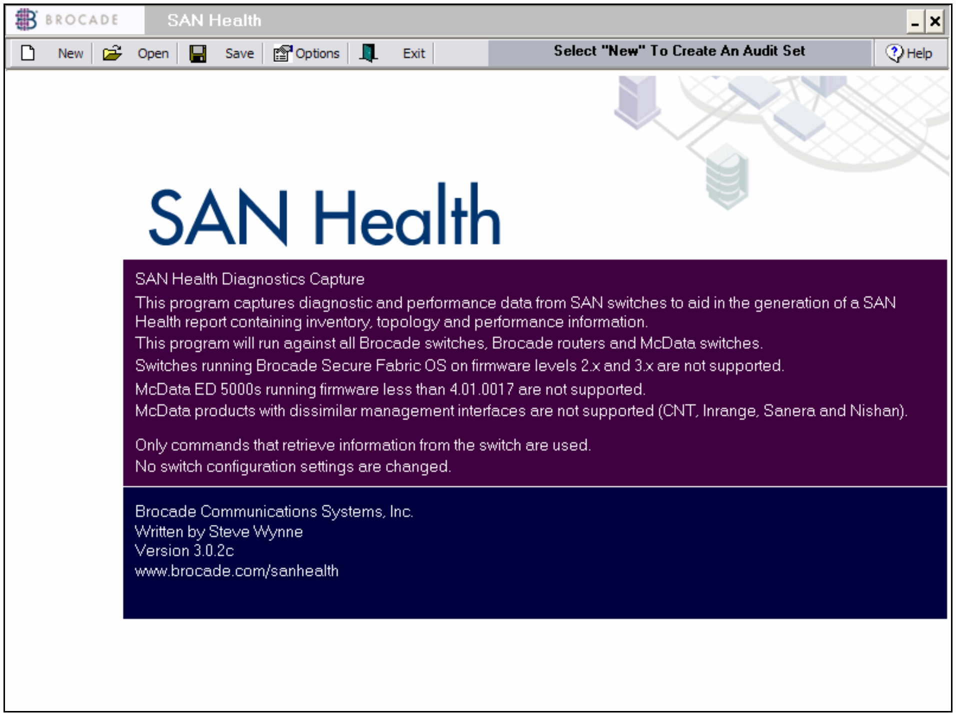
SAN Health provides a full status report on your SAN environment by the use of two mechanisms: a back-end reporting processor, and a front-end data collection agent. When the Front End (FE) has completed a scan of the SAN and collected all the appropriate data, the Back End (BE) analyzes this information for potential issues, and produces a Visio® topology diagram of the SAN. The BE report covers fabrics, switches individual ports, and historical performance graphs. It also recommends some best practice procedures.

Implementation

The Front End data collection tool (FE) can be downloaded here:

`http://www.brocade.com/support/sanhealth.jsp`

After it is downloaded, unzipped and installed, you can execute it by using the desktop icon, and you see the startup panel as shown in Figure 1-263.



SAN Health Diagnostics Capture

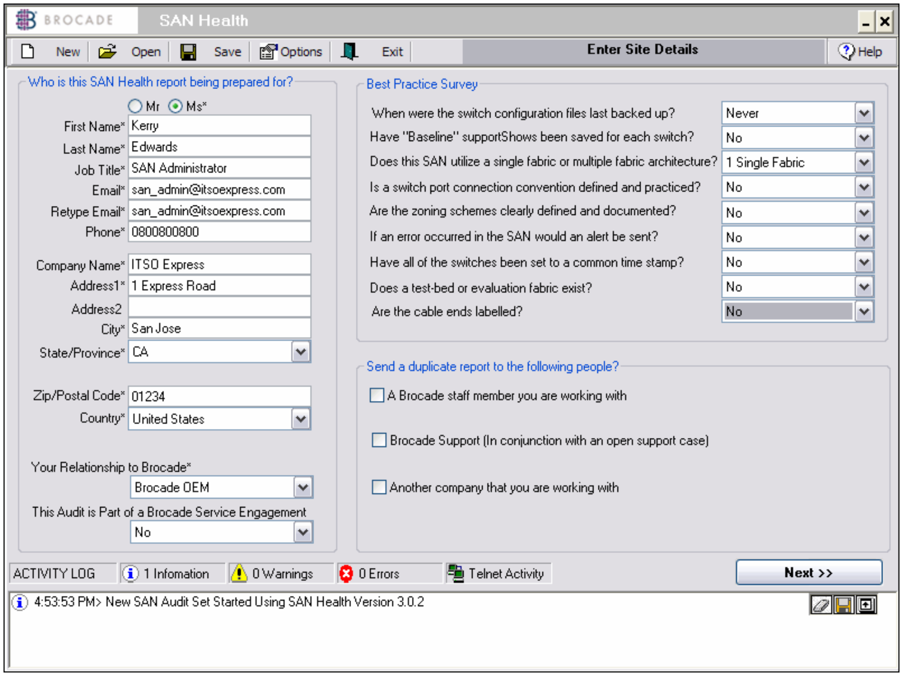
This program captures diagnostic and performance data from SAN switches to aid in the generation of a SAN Health report containing inventory, topology and performance information.
This program will run against all Brocade switches, Brocade routers and McData switches.
Switches running Brocade Secure Fabric OS on firmware levels 2.x and 3.x are not supported.
McData ED 5000s running firmware less than 4.01.0017 are not supported.
McData products with dissimilar management interfaces are not supported (CNT, Inrange, Sanera and Nishan).

Only commands that retrieve information from the switch are used.
No switch configuration settings are changed.

Brocade Communications Systems, Inc.
Written by Steve Wynne
Version 3.0.2c
www.brocade.com/sanhealth

Figure 1-263 SAN Health startup panel

First you have to answer a few questions regarding the SAN itself and how you maintain your SAN, as shown in Figure 1-264.



Who is this SAN Health report being prepared for?

○ Mr ● Ms*
First Name* Kerry
Last Name* Edwards
Job Title* SAN Administrator
Email* san_admin@itsoexpress.com
Retype Email* san_admin@itsoexpress.com
Phone* 0800800800
Company Name* ITSO Express
Address1* 1 Express Road
Address2
City* San Jose
State/Province* CA
Zip/Postal Code* 01234
Country* United States
Your Relationship to Brocade* Brocade OEM
This Audit is Part of a Brocade Service Engagement No

Best Practice Survey

When were the switch configuration files last backed up?	Never
Have "Baseline" supportShows been saved for each switch?	No
Does this SAN utilize a single fabric or multiple fabric architecture?	1 Single Fabric
Is a switch port connection convention defined and practiced?	No
Are the zoning schemes clearly defined and documented?	No
If an error occurred in the SAN would an alert be sent?	No
Have all of the switches been set to a common time stamp?	No
Does a test-bed or evaluation fabric exist?	No
Are the cable ends labelled?	No

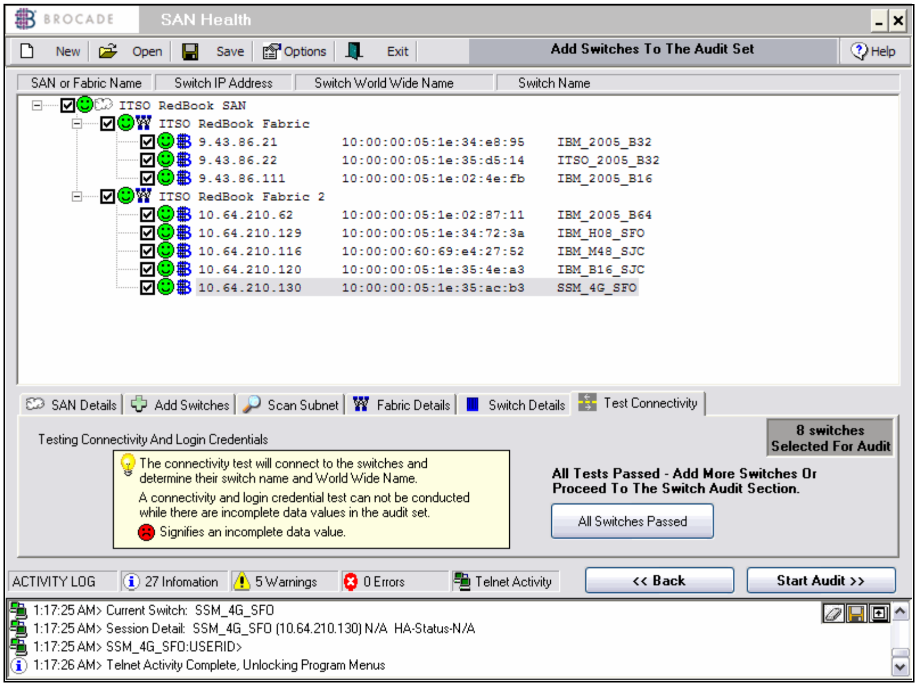
Send a duplicate report to the following people?

- ☐ A Brocade staff member you are working with
- ☐ Brocade Support (In conjunction with an open support case)
- ☐ Another company that you are working with

```
4:53:53 PM> New SAN Audit Set Started Using SAN Health Version 3.0.2
```

Figure 1-264 Personal details and how you maintain your SAN

Now you add your switches or fabrics into the data collection engine. We start by naming our SAN on the `SAN` **Details** tab. Next we add our switches using the **Add switches** tab, before moving on to the **Fabric** tab to provide the fabric details. We then complete the **Switch Details** tab before testing the connectivity as shown in Figure 1-265.


BROCADE
SAN Health
New
Open
Save
Options
Exit
Add Switches To The Audit Set
Help
SAN Details
Add Switches
Scan Subnet
Fabric Details
Switch Details
Test Connectivity
8 switches Selected For Audit
All Switches Passed
ACTIVITY LOG
27 Infomation
5 Warnings
0 Errors
Telnet Activity
<< Back
Start Audit >>

SAN or Fabric Name	Switch IP Address	Switch World Wide Name	Switch Name
☑ ITSO RedBook SAN			
☑ ITSO RedBook Fabric			
	☑ 9.43.86.21	10:00:00:05:1e:34:e8:95	IBM_2005_B32
	☑ 9.43.86.22	10:00:00:05:1e:35:d5:14	ITSO_2005_B32
	☑ 9.43.86.111	10:00:00:05:1e:02:4e:fb	IBM_2005_B16
☑ ITSO RedBook Fabric 2			
	☑ 10.64.210.62	10:00:00:05:1e:02:87:11	IBM_2005_B64
	☑ 10.64.210.129	10:00:00:05:1e:34:72:3a	IBM_H08_SFO
	☑ 10.64.210.116	10:00:00:60:69:e4:27:52	IBM_M48_SJC
	☑ 10.64.210.120	10:00:00:05:1e:35:4e:a3	IBM_B16_SJC
	☑ 10.64.210.130	10:00:00:05:1e:35:ac:b3	SSM_4G_SFO

Testing Connectivity And Login Credentials

The connectivity test will connect to the switches and determine their switch name and World Wide Name.

A connectivity and login credential test can not be conducted while there are incomplete data values in the audit set.

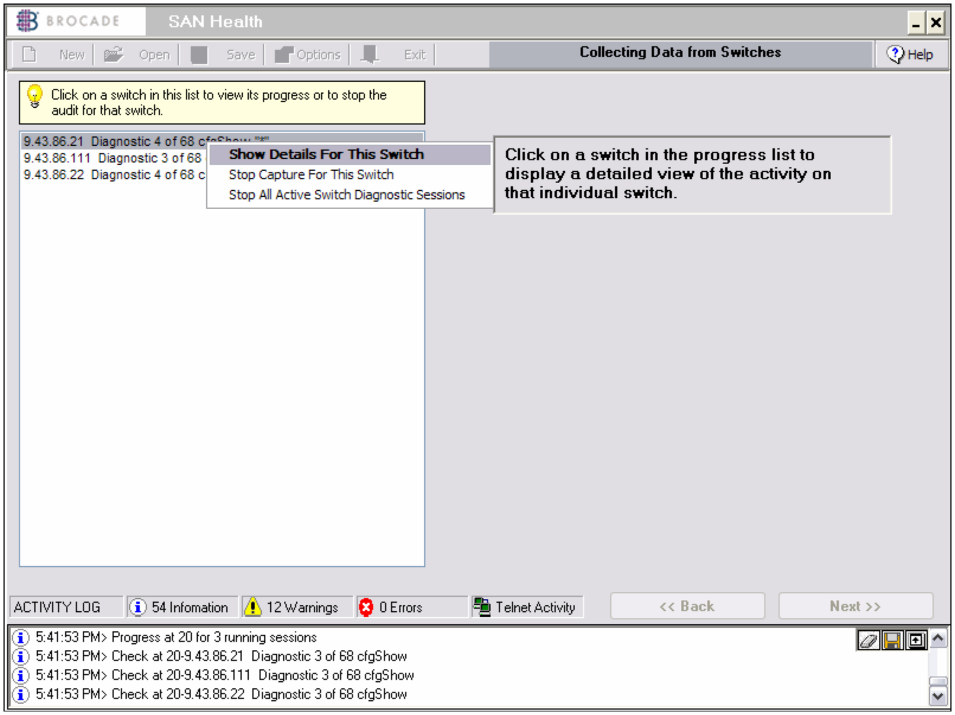
Signifies an incomplete data value.

All Tests Passed - Add More Switches Or Proceed To The Switch Audit Section.

```
1:17:25 AM> Current Switch:  SSM_4G_SFO
1:17:25 AM> Session Detail:  SSM_4G_SFO (10.64.210.130) N/A  HA-Status-N/A
1:17:25 AM> SSM_4G_SFO:USERID>
1:17:26 AM> Telnet Activity Complete, Unlocking Program Menus
```

Figure 1-265 adding switches

When this is complete, the audit begins after clicking the **`Start Audit`** button. The SAN Health now gathers data for several minutes, or longer depending upon what we chose to set the **`capture performance data interval`** to on the Fabric tab. We can watch the progress of the tool as it completes the checks. Right-clicking a specific switch allows us to view its status details. This can be seen in Figure 1-266 and Figure 1-267.


BROCADE
SAN Health
New
Open
Save
Options
Exit
Collecting Data from Switches
Help
Show Details For This Switch
Stop Capture For This Switch
Stop All Active Switch Diagnostic Sessions
ACTIVITY LOG
54 Infomation
12 Warnings
0 Errors
Telnet Activity
<< Back
Next >>

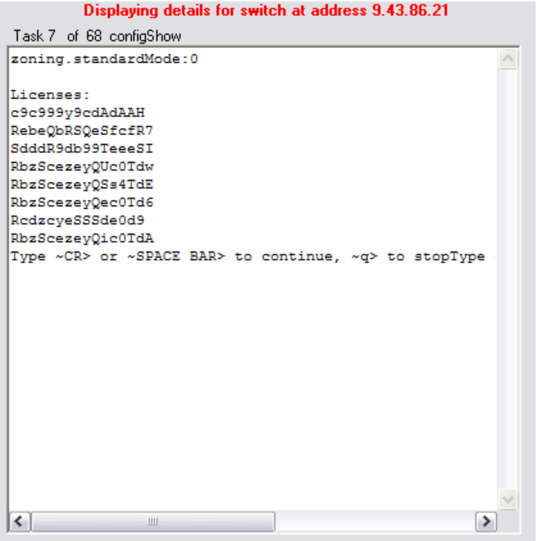
Click on a switch in this list to view its progress or to stop the audit for that switch.

```
9.43.86.21  Diagnostic 4 of 68 cfgShow "*"
9.43.86.111  Diagnostic 3 of 68
9.43.86.22  Diagnostic 4 of 68 c
```

Click on a switch in the progress list to display a detailed view of the activity on that individual switch.

```
5:41:53 PM> Progress at 20 for 3 running sessions
5:41:53 PM> Check at 20-9.43.86.21  Diagnostic 3 of 68 cfgShow
5:41:53 PM> Check at 20-9.43.86.111  Diagnostic 3 of 68 cfgShow
5:41:53 PM> Check at 20-9.43.86.22  Diagnostic 3 of 68 cfgShow
```

Figure 1-266   SAN Health viewing the status of a specific switch 1/2



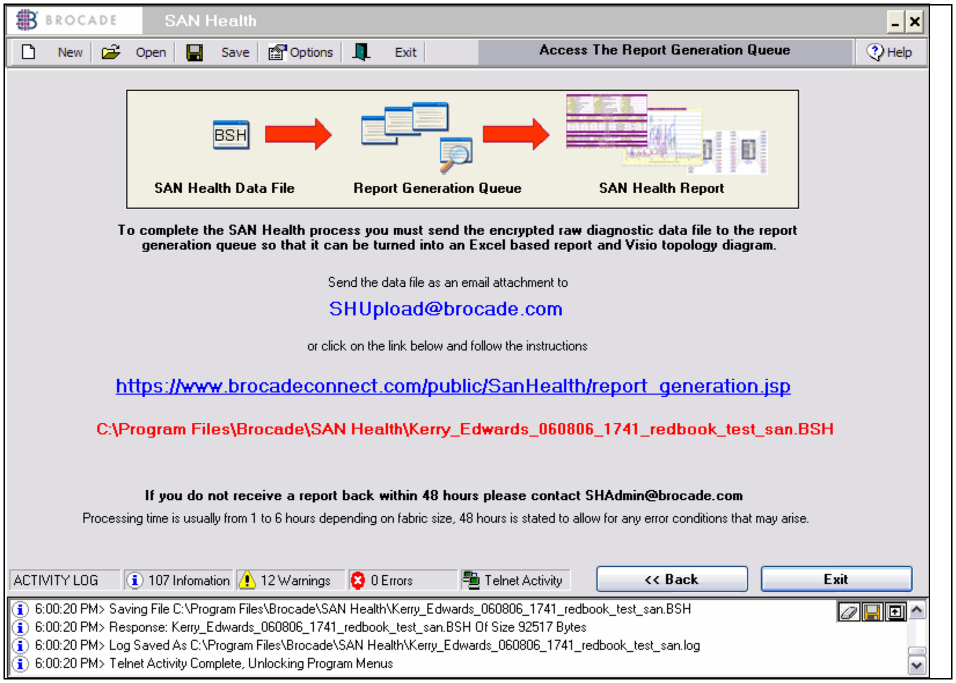
Displaying details for switch at address 9.43.86.21

Task 7 of 68 configShow

```
zoning.standardMode:0

Licenses:
c9c999y9cdAdAAH
RebeQbRSQeSfcfR7
SdddR9db99TeeeSI
RbzScezeyQUc0Tdw
RbzScezeyQSs4TdE
RbzScezeyQec0Td6
RcdzcyeSSSde0d9
RbzScezeyQic0TdA
Type ~CR> or ~SPACE BAR> to continue, ~q> to stopType
```

Figure 1-267   SAN Health viewing the status on a specific switch 2/2

When this process has completed, the output is encrypted and compressed ready for packaging into the BE data processor. On-screen instructions show how to have the output analyzed by the BE processor, as shown in Figure 1-268.


BROCADE
SAN Health
New
Open
Save
Options
Exit
Access The Report Generation Queue
Help
BSH
SAN Health Data File
Report Generation Queue
SAN Health Report
ACTIVITY LOG
107 Information
12 Warnings
0 Errors
Telnet Activity
<< Back
Exit

To complete the SAN Health process you must send the encrypted raw diagnostic data file to the report generation queue so that it can be turned into an Excel based report and Visio topology diagram.

Send the data file as an email attachment to

SHUpload@brocade.com

or click on the link below and follow the instructions

https://www.brocadeconnect.com/public/SanHealth/report_generation.jsp

C:\Program Files\Brocade\SAN Health\Kerry_Edwards_060806_1741_redbook_test_san.BSH

If you do not receive a report back within 48 hours please contact SHAdmin@brocade.com

Processing time is usually from 1 to 6 hours depending on fabric size, 48 hours is stated to allow for any error conditions that may arise.

```
6:00:20 PM> Saving File C:\Program Files\Brocade\SAN Health\Kerry_Edwards_060806_1741_redbook_test_san.BSH
6:00:20 PM> Response: Kerry_Edwards_060806_1741_redbook_test_san.BSH Of Size 92517 Bytes
6:00:20 PM> Log Saved As C:\Program Files\Brocade\SAN Health\Kerry_Edwards_060806_1741_redbook_test_san.log
6:00:20 PM> Telnet Activity Complete, Unlocking Program Menus
```

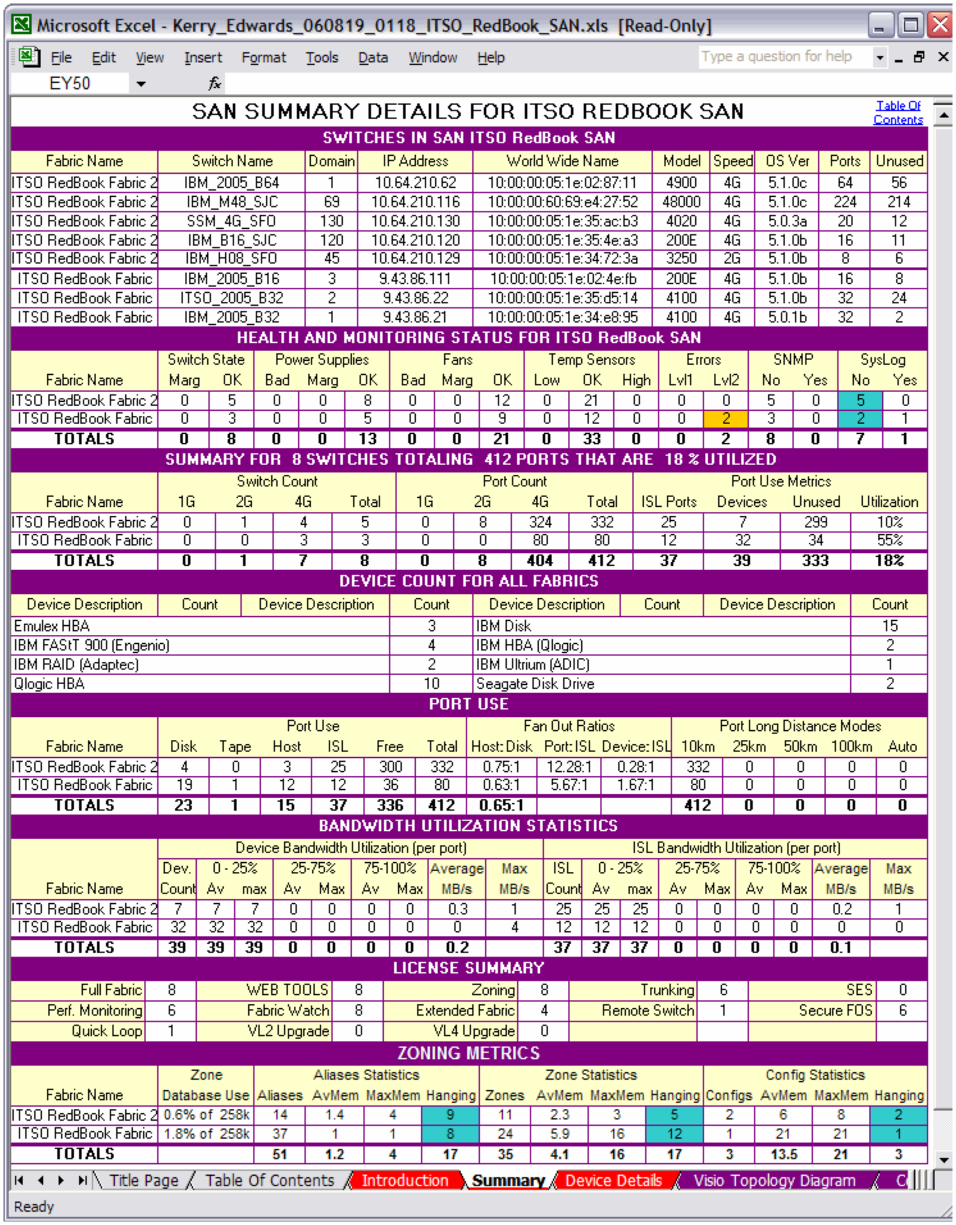
Figure 1-268 where to send the SAN Heath output

This final panel describes how to upload the results to brocade.com for BE processing. These results commonly return within 24 hours.

On their return, you receive two files. One is a Visio connection diagram of the SAN Layout. The other is a thorough SAN analysis captured into an Excel spreadsheet. You must have Excel loaded on your workstation in order to view this report.

In the following figures, we show a selection of screen captures from this report.

Figure 1-269 shows the SAN Health Summary.



SAN SUMMARY DETAILS FOR ITSO REDBOOK SAN

SWITCHES IN SAN ITSO RedBook SAN

Fabric Name	Switch Name	Domain	IP Address	World Wide Name	Model	Speed	OS Ver	Ports	Unused
ITSO RedBook Fabric 2	IBM_2005_B64	1	10.64.210.62	10:00:00:05:1e:02:87:11	4900	4G	5.1.0c	64	56
ITSO RedBook Fabric 2	IBM_M48_SJC	69	10.64.210.116	10:00:00:60:69:e4:27:52	48000	4G	5.1.0c	224	214
ITSO RedBook Fabric 2	SSM_4G_SFO	130	10.64.210.130	10:00:00:05:1e:35:ac:b3	4020	4G	5.0.3a	20	12
ITSO RedBook Fabric 2	IBM_B16_SJC	120	10.64.210.120	10:00:00:05:1e:35:4e:a3	200E	4G	5.1.0b	16	11
ITSO RedBook Fabric 2	IBM_H08_SFO	45	10.64.210.129	10:00:00:05:1e:34:72:3a	3250	2G	5.1.0b	8	6
ITSO RedBook Fabric	IBM_2005_B16	3	9.43.86.111	10:00:00:05:1e:02:4e:fb	200E	4G	5.1.0b	16	8
ITSO RedBook Fabric	ITSO_2005_B32	2	9.43.86.22	10:00:00:05:1e:35:d5:14	4100	4G	5.1.0b	32	24
ITSO RedBook Fabric	IBM_2005_B32	1	9.43.86.21	10:00:00:05:1e:34:e8:95	4100	4G	5.0.1b	32	2

HEALTH AND MONITORING STATUS FOR ITSO RedBook SAN

	Switch State		Power Supplies			Fans			Temp Sensors			Errors		SNMP		SysLog	
Fabric Name	Marg	OK	Bad	Marg	OK	Bad	Marg	OK	Low	OK	High	Lvl1	Lvl2	No	Yes	No	Yes
ITSO RedBook Fabric 2	0	5	0	0	8	0	0	12	0	21	0	0	0	5	0	5	0
ITSO RedBook Fabric	0	3	0	0	5	0	0	9	0	12	0	0	2	3	0	2	1
TOTALS	**0**	**8**	**0**	**0**	**13**	**0**	**0**	**21**	**0**	**33**	**0**	**0**	**2**	**8**	**0**	**7**	**1**

SUMMARY FOR 8 SWITCHES TOTALING 412 PORTS THAT ARE 18 % UTILIZED

	Switch Count				Port Count				Port Use Metrics			
Fabric Name	1G	2G	4G	Total	1G	2G	4G	Total	ISL Ports	Devices	Unused	Utilization
ITSO RedBook Fabric 2	0	1	4	5	0	8	324	332	25	7	299	10%
ITSO RedBook Fabric	0	0	3	3	0	0	80	80	12	32	34	55%
TOTALS	**0**	**1**	**7**	**8**	**0**	**8**	**404**	**412**	**37**	**39**	**333**	**18%**

DEVICE COUNT FOR ALL FABRICS

Device Description	Count	Device Description	Count	Device Description	Count	Device Description	Count
Emulex HBA			3	IBM Disk			15
IBM FAStT 900 (Engenio)			4	IBM HBA (Qlogic)			2
IBM RAID (Adaptec)			2	IBM Ultrium (ADIC)			1
Qlogic HBA			10	Seagate Disk Drive			2

PORT USE

	Port Use						Fan Out Ratios			Port Long Distance Modes				
Fabric Name	Disk	Tape	Host	ISL	Free	Total	Host: Disk	Port: ISL	Device: ISL	10km	25km	50km	100km	Auto
ITSO RedBook Fabric 2	4	0	3	25	300	332	0.75:1	12.28:1	0.28:1	332	0	0	0	0
ITSO RedBook Fabric	19	1	12	12	36	80	0.63:1	5.67:1	1.67:1	80	0	0	0	0
TOTALS	**23**	**1**	**15**	**37**	**336**	**412**	**0.65:1**			**412**	**0**	**0**	**0**	**0**

BANDWIDTH UTILIZATION STATISTICS

	Device Bandwidth Utilization (per port)									ISL Bandwidth Utilization (per port)								
	Dev.	0 - 25%		25-75%		75-100%		Average	Max	ISL	0 - 25%		25-75%		75-100%		Average	Max
Fabric Name	Count	Av	max	Av	Max	Av	Max	MB/s	MB/s	Count	Av	max	Av	Max	Av	Max	MB/s	MB/s
ITSO RedBook Fabric 2	7	7	7	0	0	0	0	0.3	1	25	25	25	0	0	0	0	0.2	1
ITSO RedBook Fabric	32	32	32	0	0	0	0	0	4	12	12	12	0	0	0	0	0	0
TOTALS	**39**	**39**	**39**	**0**	**0**	**0**	**0**	**0.2**		**37**	**37**	**37**	**0**	**0**	**0**	**0**	**0.1**	

LICENSE SUMMARY

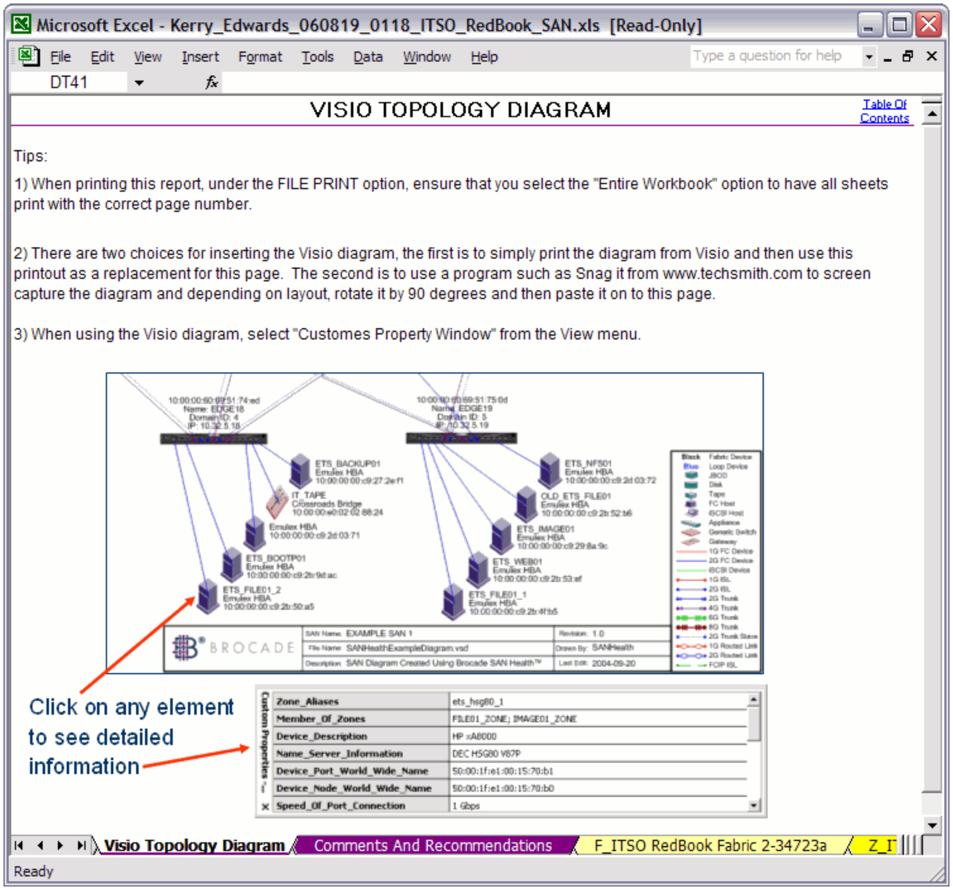
Full Fabric	8	WEB TOOLS	8	Zoning	8	Trunking	6	SES	0
Perf. Monitoring	6	Fabric Watch	8	Extended Fabric	4	Remote Switch	1	Secure FOS	6
Quick Loop	1	VL2 Upgrade	0	VL4 Upgrade	0				

ZONING METRICS

	Zone	Aliases Statistics				Zone Statistics				Config Statistics			
Fabric Name	Database Use	Aliases	AvMem	MaxMem	Hanging	Zones	AvMem	MaxMem	Hanging	Configs	AvMem	MaxMem	Hanging
ITSO RedBook Fabric 2	0.6% of 258k	14	1.4	4	9	11	2.3	3	5	2	6	8	2
ITSO RedBook Fabric	1.8% of 258k	37	1	1	8	24	5.9	16	12	1	21	21	1
TOTALS		**51**	**1.2**	**4**	**17**	**35**	**4.1**	**16**	**17**	**3**	**13.5**	**21**	**3**

Figure 1-269 SAN Health Summary

Figure 1-270 shows a copy of the Visio diagram.


Microsoft Excel - Kerry_Edwards_060819_0118_ITSO_RedBook_SAN.xls [Read-Only]
File Edit View Insert Format Tools Data Window Help
Type a question for help
DT41
fx
Table Of Contents
10:00:00:60:69:51:74:ed
Name: EDGE18
Domain ID: 4
IP: 10.32.5.18
10:00:00:60:69:51:75:0d
Name: EDGE19
Domain ID: 5
IP: 10.32.5.19
ETS_BACKUP01
Emulex HBA
10:00:00:00:c9:27:2e:f1
IT_TAPE
Crossroads Bridge
10:00:00:e0:02:02:88:24
Emulex HBA
10:00:00:00:c9:2d:03:71
ETS_BOOTP01
Emulex HBA
10:00:00:00:c9:2b:9d:ac
ETS_FILE01_2
Emulex HBA
10:00:00:00:c9:2b:50:a5
ETS_NFS01
Emulex HBA
10:00:00:00:c9:2d:03:72
OLD_ETS_FILE01
Emulex HBA
10:00:00:00:c9:2b:52:b6
ETS_IMAGE01
Emulex HBA
10:00:00:00:c9:29:8a:9c
ETS_WEB01
Emulex HBA
10:00:00:00:c9:2b:53:ef
ETS_FILE01_1
Emulex HBA
10:00:00:00:c9:2b:4f:b5
Black Fabric Device
Blue Loop Device
JBOD
Disk
Tape
FC Host
iSCSI Host
Appliance
Generic Switch
Gateway
1G FC Device
2G FC Device
iSCSI Device
1G ISL
2G ISL
2G Trunk
4G Trunk
6G Trunk
8G Trunk
2G Trunk Slave
1G Routed Link
2G Routed Link
FCIP ISL
BROCADE
SAN Name: EXAMPLE SAN 1
File Name: SANHealthExampleDiagram.vsd
Description: SAN Diagram Created Using Brocade SAN Health™
Revision: 1.0
Drawn By: SANHealth
Last Edit: 2004-09-20
Custom Properties
Visio Topology Diagram
Comments And Recommendations
F_ITSO RedBook Fabric 2-34723a
Z_I
Ready

VISIO TOPOLOGY DIAGRAM

Tips:

1) When printing this report, under the FILE PRINT option, ensure that you select the "Entire Workbook" option to have all sheets print with the correct page number.

2) There are two choices for inserting the Visio diagram, the first is to simply print the diagram from Visio and then use this printout as a replacement for this page. The second is to use a program such as Snag it from www.techsmith.com to screen capture the diagram and depending on layout, rotate it by 90 degrees and then paste it on to this page.

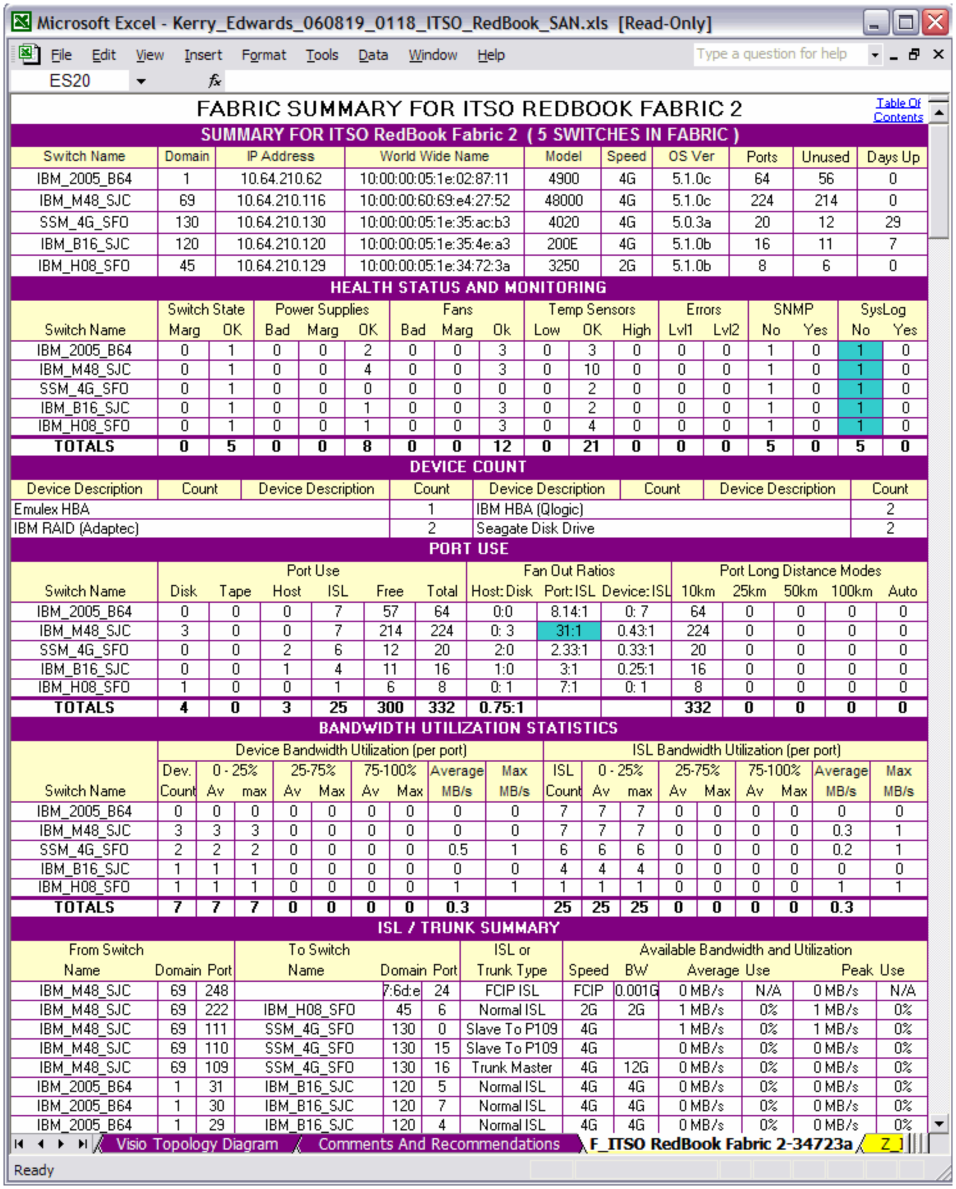
3) When using the Visio diagram, select "Customes Property Window" from the View menu.

Click on any element to see detailed information

Zone_Aliases	ets_hsg80_1
Member_Of_Zones	FILE01_ZONE; IMAGE01_ZONE
Device_Description	HP xA8000
Name_Server_Information	DEC HSG80 V87P
Device_Port_World_Wide_Name	50:00:1f:e1:00:15:70:b1
Device_Node_World_Wide_Name	50:00:1f:e1:00:15:70:b0
Speed_Of_Port_Connection	1 Gbps

Figure 1-270 SAN Health Visio diagram

Figure 1-271 shows a fabric specific summary.


Microsoft Excel - Kerry_Edwards_060819_0118_ITSO_RedBook_SAN.xls [Read-Only]
File
Edit
View
Insert
Format
Tools
Data
Window
Help
Type a question for help
ES20
fx
Table Of Contents
Visio Topology Diagram
Comments And Recommendations
F_ITSO RedBook Fabric 2-34723a
Z_1
Ready

FABRIC SUMMARY FOR ITSO REDBOOK FABRIC 2

SUMMARY FOR ITSO RedBook Fabric 2 (5 SWITCHES IN FABRIC)

Switch Name	Domain	IP Address	World Wide Name	Model	Speed	OS Ver	Ports	Unused	Days Up
IBM_2005_B64	1	10.64.210.62	10:00:00:05:1e:02:87:11	4900	4G	5.1.0c	64	56	0
IBM_M48_SJC	69	10.64.210.116	10:00:00:60:69:e4:27:52	48000	4G	5.1.0c	224	214	0
SSM_4G_SFO	130	10.64.210.130	10:00:00:05:1e:35:ac:b3	4020	4G	5.0.3a	20	12	29
IBM_B16_SJC	120	10.64.210.120	10:00:00:05:1e:35:4e:a3	200E	4G	5.1.0b	16	11	7
IBM_H08_SFO	45	10.64.210.129	10:00:00:05:1e:34:72:3a	3250	2G	5.1.0b	8	6	0

HEALTH STATUS AND MONITORING

	Switch State		Power Supplies			Fans			Temp Sensors			Errors		SNMP		SysLog	
Switch Name	Marg	OK	Bad	Marg	OK	Bad	Marg	Ok	Low	OK	High	Lvl1	Lvl2	No	Yes	No	Yes
IBM_2005_B64	0	1	0	0	2	0	0	3	0	3	0	0	0	1	0	1	0
IBM_M48_SJC	0	1	0	0	4	0	0	3	0	10	0	0	0	1	0	1	0
SSM_4G_SFO	0	1	0	0	0	0	0	0	0	2	0	0	0	1	0	1	0
IBM_B16_SJC	0	1	0	0	1	0	0	3	0	2	0	0	0	1	0	1	0
IBM_H08_SFO	0	1	0	0	1	0	0	3	0	4	0	0	0	1	0	1	0
TOTALS	**0**	**5**	**0**	**0**	**8**	**0**	**0**	**12**	**0**	**21**	**0**	**0**	**0**	**5**	**0**	**5**	**0**

DEVICE COUNT

Device Description	Count	Device Description	Count	Device Description	Count	Device Description	Count
Emulex HBA			1	IBM HBA (Qlogic)			2
IBM RAID (Adaptec)			2	Seagate Disk Drive			2

PORT USE

	Port Use						Fan Out Ratios			Port Long Distance Modes				
Switch Name	Disk	Tape	Host	ISL	Free	Total	Host: Disk	Port: ISL	Device: ISL	10km	25km	50km	100km	Auto
IBM_2005_B64	0	0	0	7	57	64	0:0	8.14:1	0: 7	64	0	0	0	0
IBM_M48_SJC	3	0	0	7	214	224	0: 3	31:1	0.43:1	224	0	0	0	0
SSM_4G_SFO	0	0	2	6	12	20	2:0	2.33:1	0.33:1	20	0	0	0	0
IBM_B16_SJC	0	0	1	4	11	16	1:0	3:1	0.25:1	16	0	0	0	0
IBM_H08_SFO	1	0	0	1	6	8	0: 1	7:1	0: 1	8	0	0	0	0
TOTALS	**4**	**0**	**3**	**25**	**300**	**332**	**0.75:1**			**332**	**0**	**0**	**0**	**0**

BANDWIDTH UTILIZATION STATISTICS

	Device Bandwidth Utilization (per port)									ISL Bandwidth Utilization (per port)								
	Dev.	0 - 25%		25-75%		75-100%		Average	Max	ISL	0 - 25%		25-75%		75-100%		Average	Max
Switch Name	Count	Av	max	Av	Max	Av	Max	MB/s	MB/s	Count	Av	max	Av	Max	Av	Max	MB/s	MB/s
IBM_2005_B64	0	0	0	0	0	0	0	0	0	7	7	7	0	0	0	0	0	0
IBM_M48_SJC	3	3	3	0	0	0	0	0	0	7	7	7	0	0	0	0	0.3	1
SSM_4G_SFO	2	2	2	0	0	0	0	0.5	1	6	6	6	0	0	0	0	0.2	1
IBM_B16_SJC	1	1	1	0	0	0	0	0	0	4	4	4	0	0	0	0	0	0
IBM_H08_SFO	1	1	1	0	0	0	0	1	1	1	1	1	0	0	0	0	1	1
TOTALS	**7**	**7**	**7**	**0**	**0**	**0**	**0**	**0.3**		**25**	**25**	**25**	**0**	**0**	**0**	**0**	**0.3**	

ISL / TRUNK SUMMARY

From Switch			To Switch			ISL or	Available Bandwidth and Utilization					
Name	Domain	Port	Name	Domain	Port	Trunk Type	Speed	BW	Average Use		Peak Use	
IBM_M48_SJC	69	248		7:6d:e	24	FCIP ISL	FCIP	0.001G	0 MB/s	N/A	0 MB/s	N/A
IBM_M48_SJC	69	222	IBM_H08_SFO	45	6	Normal ISL	2G	2G	1 MB/s	0%	1 MB/s	0%
IBM_M48_SJC	69	111	SSM_4G_SFO	130	0	Slave To P109	4G		1 MB/s	0%	1 MB/s	0%
IBM_M48_SJC	69	110	SSM_4G_SFO	130	15	Slave To P109	4G		0 MB/s	0%	0 MB/s	0%
IBM_M48_SJC	69	109	SSM_4G_SFO	130	16	Trunk Master	4G	12G	0 MB/s	0%	0 MB/s	0%
IBM_2005_B64	1	31	IBM_B16_SJC	120	5	Normal ISL	4G	4G	0 MB/s	0%	0 MB/s	0%
IBM_2005_B64	1	30	IBM_B16_SJC	120	7	Normal ISL	4G	4G	0 MB/s	0%	0 MB/s	0%
IBM_2005_B64	1	29	IBM_B16_SJC	120	4	Normal ISL	4G	4G	0 MB/s	0%	0 MB/s	0%

Figure 1-271 A fabric specific summary

1.10.2 Error logs

The b-type family of switches provide multiple sources of errors logs and debug data. These can be collected from WebTools, CLI, or via automated tools that run when the switch experiences a critical problem.

Some of these logs are:

- **`TraceDump:`** The switch dumps a copy of its memory and pointers into a trace file.
- **`RASLOG:`** This log contains debug data from the switch.
- **`supportshow:`** This is configuration and status information from the switch.

Capturing a trace dump

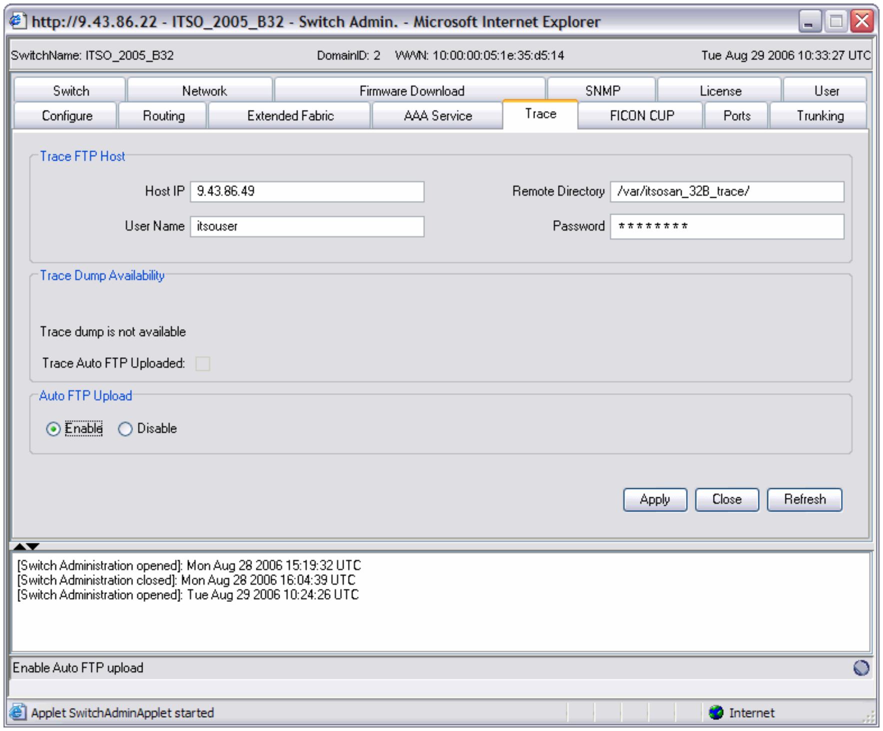
When a switch “panics”, dependent upon the circumstances, it might produce a trace dump. This can be automatically uploaded to an FTP server when the switch recovers from this failure.

From within the WebTools Admin interface, the **Trace** tab allows us to view and configure the FTP host target, enable/disable automatic trace uploads and manually update a trace dump as shown in Figure 1-272.

Tracing is always “on” and generates a trace dump whenever there are certain actions within the switch; for example, if:

- It is triggered manually through the **`traceDump`** command.
- A critical level log message occurs.
- A particular log message occurs because the **traceTrig** command has been used.
- A kernel panic occurs.
- A hardware watchdog timer expires.

The trace dump is maintained on the switch until it is uploaded via FTP, or until another trace dump is generated. Be aware that a new trace dump overwrites the previous trace dump.


http://9.43.86.22 - ITSO_2005_B32 - Switch Admin. - Microsoft Internet Explorer
Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Ports
Trunking
Trace FTP Host
Trace Dump Availability
Auto FTP Upload
Apply
Close
Refresh
Internet

SwitchName: ITSO_2005_B32 DomainID: 2 WWN: 10:00:00:05:1e:35:d5:14 Tue Aug 29 2006 10:33:27 UTC

Host IP: 9.43.86.49

Remote Directory: /var/itsosan_32B_trace/

User Name: itsouser

Password: ********

Trace dump is not available

Trace Auto FTP Uploaded: ☐

● Enable ○ Disable

```
[Switch Administration opened]: Mon Aug 28 2006 15:19:32 UTC
[Switch Administration closed]: Mon Aug 28 2006 16:04:39 UTC
[Switch Administration opened]: Tue Aug 29 2006 10:24:26 UTC
```

Enable Auto FTP upload

Applet SwitchAdminApplet started

Figure 1-272 Trace

SupportSave

This command allows the manual upload of the following logs to an FTP server:

- RASLOG
- TRACEdump
- supportshow
- zone log
- RCS command log
- NS event log
- FSPF status log
- Any memory CORE files.

The command structure, from the CLI is as follows:

```
supportsave [-n] [-c] [-u user_name -p password] -h host_ip -d remote_dir
```

These logs should now be sent through to your SAN hardware support team at IBM for further diagnosis.

1.11 FICON

IBM Fibre Connections (FICON) is an industry-standard, high-speed input/output (I/O) interface for mainframe connections to storage devices. FICON switching is supported by IBM TotalStorage SAN-32B switch and the SAN256B director, with support for the SAN-64B and the SAN-18BR in process at the time of writing.

1.11.1 FICON servers

Native FICON is automatically supported on Fabric OS 5.0.1 and above for IBM TotalStorage SAN256B director and IBM TotalStorage SAN32B fabric switch.

1.11.2 Intermixed FICON and FCP

FICON intermix allows you to run together both FICON and FCP through a shared director-class IBM TotalStorage SAN Switch.

1.11.3 Cascaded FICON and CUP support

FICON support of cascaded directors means that a Native FICON (FC) channel or a FICON CTC can connect a server to a device or other server via two same-vendor directors. Only a two-switch, single-hop configuration is supported.

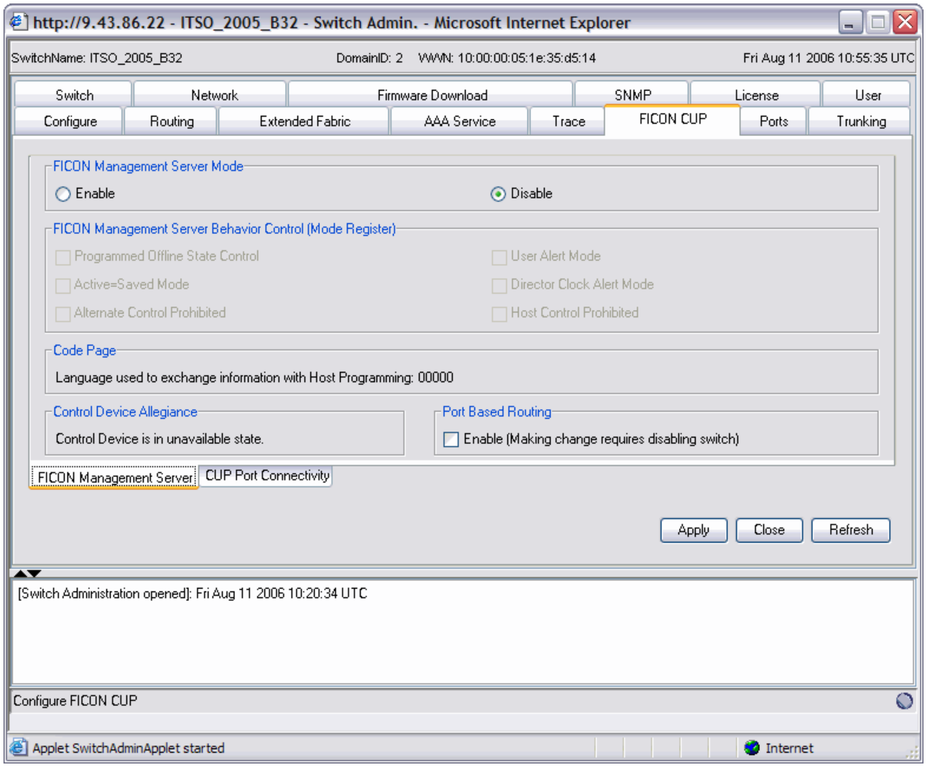
To enable Cascaded FICON support function, you have to install the Secure Fabric OS license. Cascaded FICON support is available in two directors per fabric.

The FICON Management Server (FMS) is used to support switch management using Control Unit Port (CUP). The CUP protocol is used by IBM mainframe management programs to provide in-band management for FICON switches. To use this feature, you have to install the FICON with CUP license.

To be able to use the CUP functionality, all switches in the fabric must have FICON Management Server mode (FMS mode) enabled. FICON Management Server mode is a per switch setting. After FICON Management Server mode is enabled, you can activate a CUP license without rebooting the director.

Next, we briefly discuss some of the basic functions on the FICON CUP tab. For complete information, refer to the *Brocade Web Tools Administrator's Guide*, 53-1000049-02.

From within the Admin section of WebTools, the first subtab under FICON CUP tab is where we enable the FICON Management Server mode, as shown in Figure 1-273.



http://9.43.86.22 - ITSO_2005_B32 - Switch Admin. - Microsoft Internet Explorer
Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Ports
Trunking
FICON Management Server
CUP Port Connectivity
Apply
Close
Refresh
Configure FICON CUP
Applet SwitchAdminApplet started
Internet

SwitchName: ITSO_2005_B32 DomainID: 2 WWN: 10:00:00:05:1e:35:d5:14 Fri Aug 11 2006 10:55:35 UTC

FICON Management Server Mode

○ Enable ● Disable

FICON Management Server Behavior Control (Mode Register)

☐ Programmed Offline State Control
☐ Active=Saved Mode
☐ Alternate Control Prohibited
☐ User Alert Mode
☐ Director Clock Alert Mode
☐ Host Control Prohibited

Code Page

Language used to exchange information with Host Programming: 00000

Control Device Allegiance

Control Device is in unavailable state.

Port Based Routing

☐ Enable (Making change requires disabling switch)

[Switch Administration opened]: Fri Aug 11 2006 10:20:34 UTC

Figure 1-273 FICON CUP tab1

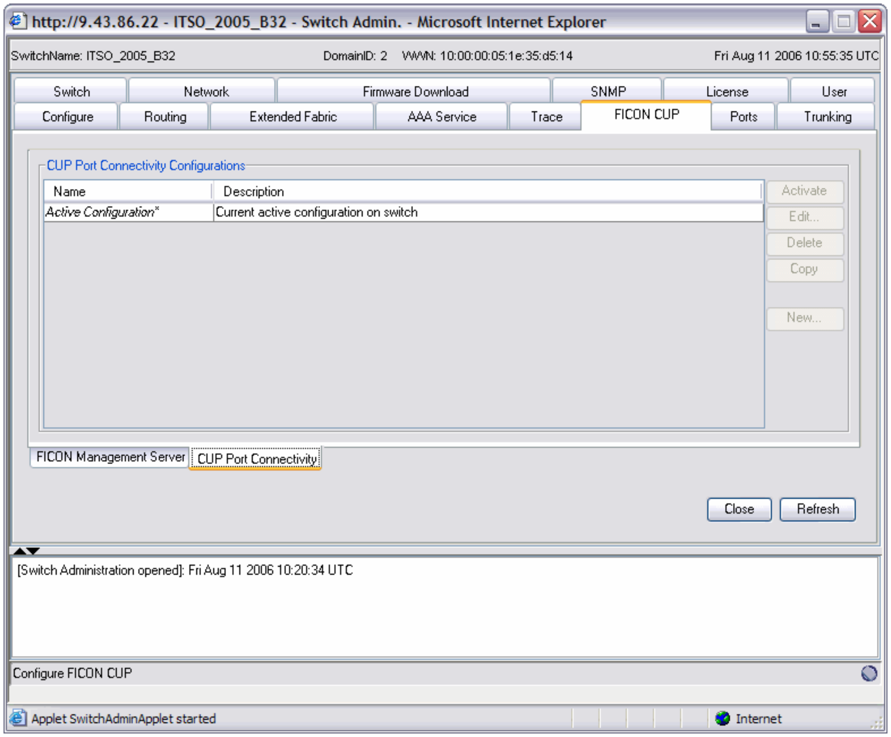
The first section determines the mode of the FICON Management server, either enabled or disabled.

The next section is entitled FICON Management Server Behavior Control and has some default settings already defined.

The Code Page section displays what language is used to exchange information with Host Programming.

The Control Device is in a default neutral state. When it is neutral, the Control Device accepts commands from any channel that has established a logical path with it and accepts commands from alternate managers. When the Control Device is switched, it establishes a logical path and accepts commands only from that logical path (device allegiance).

When the FICON Management Server is enabled, we go to the CUP port connectivity subtab to configure the ports as shown in Figure 1-274.


http://9.43.86.22 - ITSO_2005_B32 - Switch Admin. - Microsoft Internet Explorer
Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Ports
Trunking
CUP Port Connectivity Configurations
Activate
Edit...
Delete
Copy
New...
FICON Management Server
CUP Port Connectivity
Close
Refresh
Configure FICON CUP
Applet SwitchAdminApplet started
Internet

SwitchName: ITSO_2005_B32
DomainID: 2
WWN: 10:00:00:05:1e:35:d5:14
Fri Aug 11 2006 10:55:35 UTC

Name	Description
*Active Configuration**	Current active configuration on switch

```
[Switch Administration opened]: Fri Aug 11 2006 10:20:34 UTC
```

Figure 1-274 FICON tab Configure CUP connectivity

The **CUP Port Connectivity** subtab shown in Figure 1-274 has a default view which displays the CUP configuration list.

The functions on this tab are:

Activate	Activate a configuration
Edit	Modify an existing configuration (that is inactive)
Delete	Delete a configuration
Copy	Copy a configuration
New	Create a new configuration

1.12 FICON quickstart

In this topic we discuss the basic steps for configuring a switch for FICON in both a switched point-to-point and cascaded configuration.

We describe some basic FICON/mainframe steps that you must perform. It is not our intent to show any of the steps on the mainframe; however, we highlight the main considerations.

1.13 Hardware Configuration Definition

An I/O configuration defines the hardware resources available to the operating system and the connections between these resources. The resources include:

- Channels
- ESCON/FICON Directors (switches)
- Control units
- Devices

You must define an I/O configuration to the operating system (software) and the channel subsystem (hardware). The Hardware Configuration Definition (HCD) element of z/OS® combines hardware and software I/O configuration under a single interactive end-user interface. The HCD also performs validation checking which helps to eliminate errors before you attempt to use the I/O configuration.

The output of the HCD is an I/O definition file (IODF). An IODF is used to define multiple hardware and software configurations to the z/OS operating system. When you activate an IODF, the HCD defines the I/O configuration to the channel subsystem and/or the operating system. With the HCD activate function or the **`MVS™ ACTIVATE`** operator command, you can make changes to the current configuration without having to perform an initial program load (IPL) the software or power-on reset (POR) the hardware. Making changes while the system is running is known as dynamic configuration or dynamic reconfiguration.

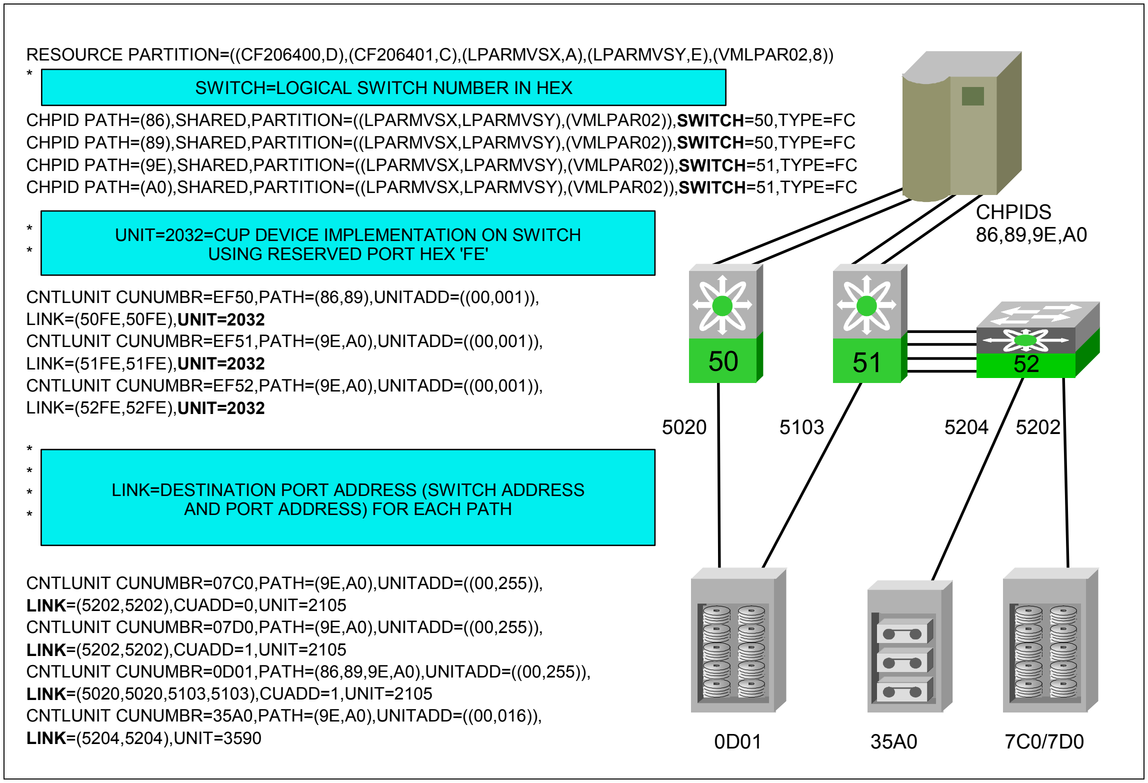
You select your I/O configuration when you:

- Do a POR.
- Do an IPL.
- Activate a dynamic configuration change.

IPL and activation require that you identify the IODF that contains the definition of your configuration. A data set called an I/O configuration data set (IOCDS) is used at POR. An IOCDS can be created from a configuration definition in an IODF. The IOCDS contains the configuration for a specific processor, while the IODF contains configuration data for multiple processors.

Important: It is highly recommended that you complete the FICON configuration on the switches before attempting to bring any CHPIDs or Control Units online, and switch configuration cannot be finished until HCD configuration is complete.

We show an example topology using double byte addressing on all three directors, and associated statements in Figure 1-275.



```
RESOURCE PARTITION=((CF206400,D),(CF206401,C),(LPARMVSX,A),(LPARMVSY,E),(VMLPAR02,8))
*   SWITCH=LOGICAL SWITCH NUMBER IN HEX
CHPID PATH=(86),SHARED,PARTITION=((LPARMVSX,LPARMVSY),(VMLPAR02)),SWITCH=50,TYPE=FC
CHPID PATH=(89),SHARED,PARTITION=((LPARMVSX,LPARMVSY),(VMLPAR02)),SWITCH=50,TYPE=FC
CHPID PATH=(9E),SHARED,PARTITION=((LPARMVSX,LPARMVSY),(VMLPAR02)),SWITCH=51,TYPE=FC
CHPID PATH=(A0),SHARED,PARTITION=((LPARMVSX,LPARMVSY),(VMLPAR02)),SWITCH=51,TYPE=FC

*   UNIT=2032=CUP DEVICE IMPLEMENTATION ON SWITCH
*   USING RESERVED PORT HEX 'FE'

CNTLUNIT CUNUMBR=EF50,PATH=(86,89),UNITADD=((00,001)),
LINK=(50FE,50FE),UNIT=2032
CNTLUNIT CUNUMBR=EF51,PATH=(9E,A0),UNITADD=((00,001)),
LINK=(51FE,51FE),UNIT=2032
CNTLUNIT CUNUMBR=EF52,PATH=(9E,A0),UNITADD=((00,001)),
LINK=(52FE,52FE),UNIT=2032

*
*   LINK=DESTINATION PORT ADDRESS (SWITCH ADDRESS
*   AND PORT ADDRESS) FOR EACH PATH
*

CNTLUNIT CUNUMBR=07C0,PATH=(9E,A0),UNITADD=((00,255)),
LINK=(5202,5202),CUADD=0,UNIT=2105
CNTLUNIT CUNUMBR=07D0,PATH=(9E,A0),UNITADD=((00,255)),
LINK=(5202,5202),CUADD=1,UNIT=2105
CNTLUNIT CUNUMBR=0D01,PATH=(86,89,9E,A0),UNITADD=((00,255)),
LINK=(5020,5020,5103,5103),CUADD=1,UNIT=2105
CNTLUNIT CUNUMBR=35A0,PATH=(9E,A0),UNITADD=((00,016)),
LINK=(5204,5204),UNIT=3590
```

Figure 1-275 FICON environment IOCP definitions

Note: There is no change to the IODEVICE or ID statements to support SAN.

We do not propose to cover the HCD definition process, because you must be familiar with that before attempting to code any of the statements shown in Figure 1-275.

For more information on FICON, we recommend the Redbooks publication, *FICON Implementation Guide*, SG24-6497, and we refer you to:

`http://www.redbooks.ibm.com/abstracts/sg246497.html?Open`

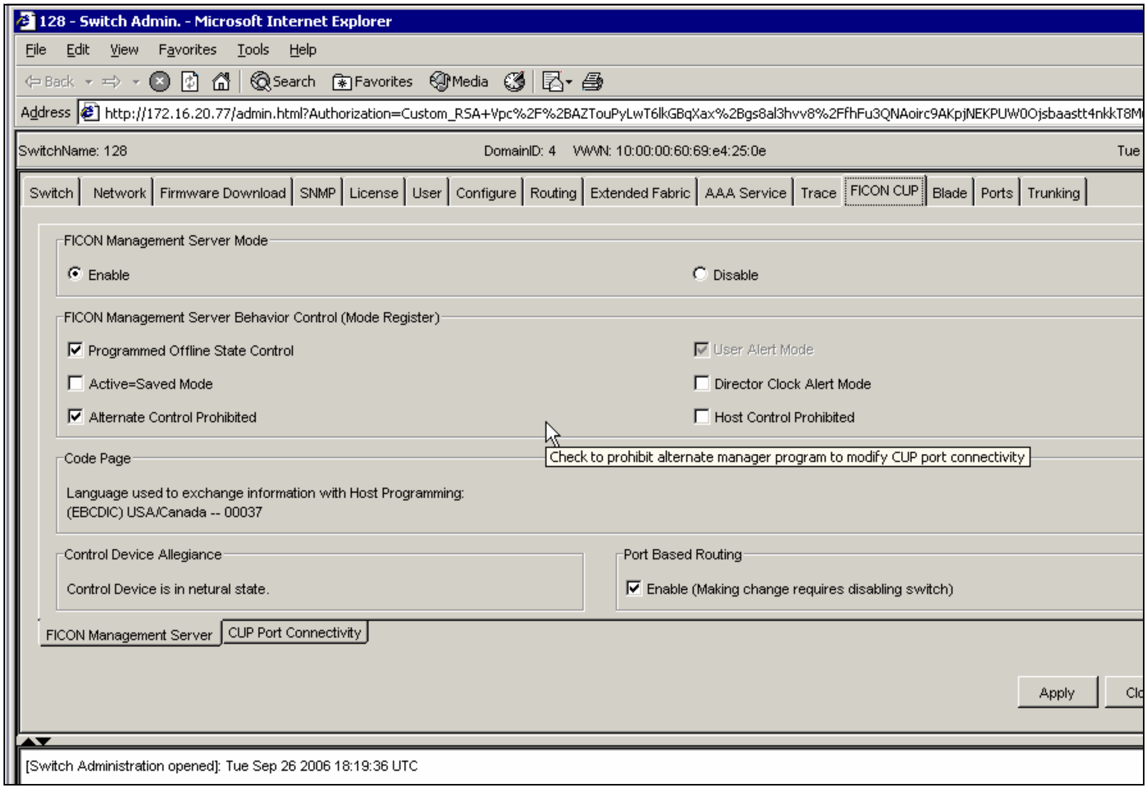
1.13.1 Configure the routing policy

Configuring the routing policy is only necessary for Condor ASIC based products. Port-based path selection is a routing policy in which paths are chosen based on ingress port and destination only. This also includes user-configured paths.

All switches with FICON devices attached must have port-based routing policy enabled. Port-based routing is a per switch routing policy. After port-based routing is enabled, you can continue with the rest of the FICON implementation.

To enable or disable port-based routing:

1. Click a switch with FICON devices attached from the Fabric Tree.
2. Launch the Switch Admin module as described on page 3-3.
3. Click the **FICON CUP** tab.
4. The FICON CUP tabbed page displays, with the FICON Management Server subtabbed page in front, as shown in Figure 1-276.
5. Check the **Enable** box in the Port Based Routing section to enable the port-based routing policy. Uncheck this box to disable port-based routing.
6. Click **Apply** to save your changes.


128 - Switch Admin. - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Switch Network Firmware Download SNMP License User Configure Routing Extended Fabric AAA Service Trace FICON CUP Blade Ports Trunking
FICON Management Server
CUP Port Connectivity
Apply

Address: http://172.16.20.77/admin.html?Authorization=Custom_RSA+Vpc%2F%2BAZTouPyLwT6lkGBqXax%2Bgs8al3hvv8%2FfhFu3QNAoirc9AKpjNEKPUW0Ojsbaastt4nkkT8M

SwitchName: 128 DomainID: 4 WWN: 10:00:00:60:69:e4:25:0e Tue

FICON Management Server Mode

● Enable ○ Disable

FICON Management Server Behavior Control (Mode Register)

- ☑ Programmed Offline State Control
- ☐ Active=Saved Mode
- ☑ Alternate Control Prohibited
- ☑ User Alert Mode
- ☐ Director Clock Alert Mode
- ☐ Host Control Prohibited

Check to prohibit alternate manager program to modify CUP port connectivity

Code Page

Language used to exchange information with Host Programming:
(EBCDIC) USA/Canada -- 00037

Control Device Allegiance

Control Device is in netural state.

Port Based Routing

☑ Enable (Making change requires disabling switch)

[Switch Administration opened]: Tue Sep 26 2006 18:19:36 UTC

Figure 1-276 Enable port routing

Enabling port-based routing means that all frames received on an ingress port destined for a destination domain are guaranteed to exit the switch in the same order in which they were received.

1.13.2 Disabling Dynamic Load Sharing

If Dynamic Load Sharing (DLS) is enabled, traffic on existing ISL ports might be affected when one or more new ISLs is added between the same two switches. Specifically, adding the new ISL might result in dropped frames as routes are adjusted to take advantage of the bandwidth provided.

By disabling DLS, you ensure that there will be no dropped frames. A similar situation occurs when an ISL port is taken offline and then brought back online. When the ISL port goes offline, the traffic on that port is rerouted to another ISL with a common destination. When the ISL port comes back online and DLS is enabled, the rerouting of traffic back to the ISL port might result in dropped frames. If DLS is not enabled, traffic is not routed back.

Currently it has to be disabled (or also enabled) via the CLI as shown in Example 1-51.

Example 1-51 dlsreset

```
128:admin> dlsshow

DLS is set

128:admin> dlsreset
128:admin> dlsshow

DLS is not set

128:admin>
```

FICON requires that DLS is *not* set.

1.13.3 Configuring In-Order Delivery

The order of delivery of frames is maintained within a switch and determined by the routing policy in effect. Following are the frame delivery behaviors for each routing policy.

- Port-based routing:

  All frames received on an ingress port destined for a destination domain are guaranteed to exit the switch in the same order in which they were received.

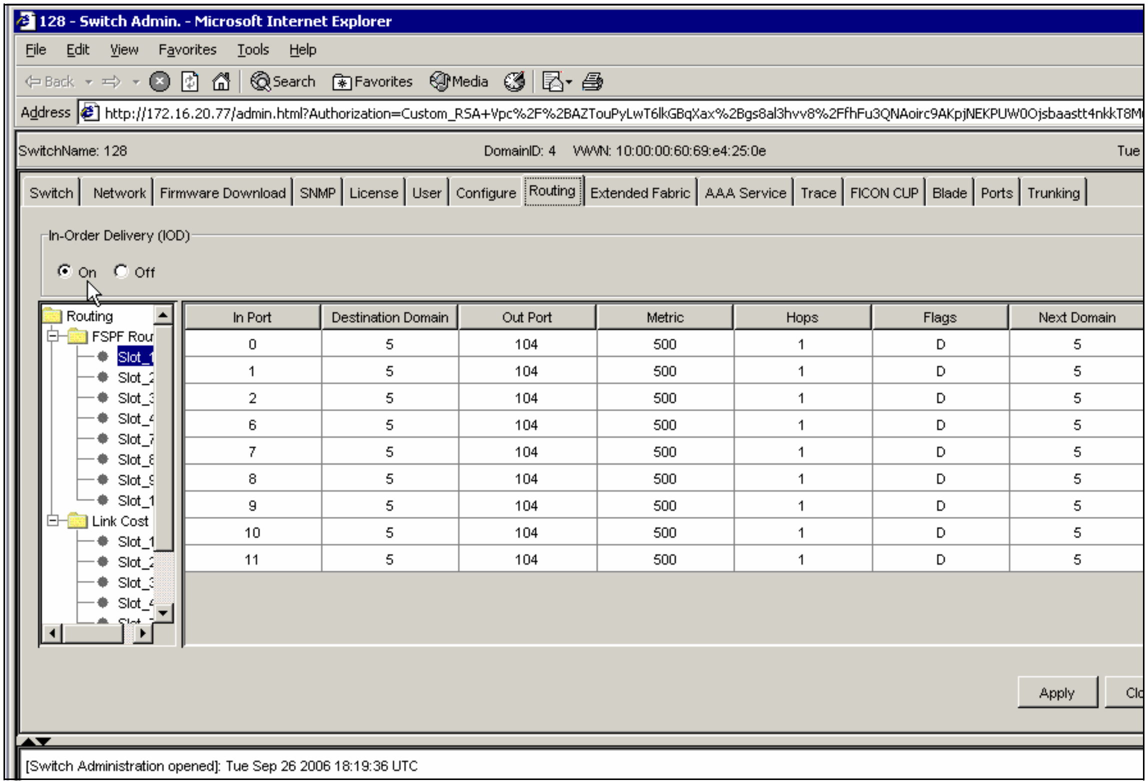
- Exchange-based routing:

  All frames received on an ingress port for a given exchange are guaranteed to exit the switch in the same order in which they were received. Because different paths are chosen for different exchanges, this policy does not maintain the order of frames across exchanges.

If even one switch in the fabric delivers out-of-order exchanges, then exchanges are delivered to the target out-of-order, regardless of the policy configured on other switches in the fabric.

Port-based routing is required for FICON.

To configure In-Order Delivery, select the **Routing** tab from Switch Admin as shown in Figure 1-277.


128 - Switch Admin. - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Switch Network Firmware Download SNMP License User Configure Routing Extended Fabric AAA Service Trace FICON CUP Blade Ports Trunking
Routing
FSPF Rou
Slot_1
Slot_2
Slot_3
Slot_4
Slot_7
Slot_8
Slot_9
Slot_1
Link Cost
Slot_1
Slot_2
Slot_3
Slot_4
Apply
Cl

Address: http://172.16.20.77/admin.html?Authorization=Custom_RSA+Vpc%2F%2BAZTouPyLwT6lkGBqXax%2Bgs8al3hvv8%2FfhFu3QNAoirc9AKpjNEKPUW0Ojsbaastt4nkkT8M

SwitchName: 128 DomainID: 4 WWN: 10:00:00:60:69:e4:25:0e Tue

In-Order Delivery (IOD)

● On ○ Off

In Port	Destination Domain	Out Port	Metric	Hops	Flags	Next Domain
0	5	104	500	1	D	5
1	5	104	500	1	D	5
2	5	104	500	1	D	5
6	5	104	500	1	D	5
7	5	104	500	1	D	5
8	5	104	500	1	D	5
9	5	104	500	1	D	5
10	5	104	500	1	D	5
11	5	104	500	1	D	5

[Switch Administration opened]: Tue Sep 26 2006 18:19:36 UTC

Figure 1-277 In-Order Delivery

In-Order Delivery is now set.

1.13.4 Configuring Domain ID and Insistent Domain ID

In a cascaded configuration, each switch must have a unique domain ID, and insistent domain ID (IDID) mode must be enabled.

When insistent domain ID (IDID) mode is enabled, the current domain setting for the switch is insistent; that is, the same ID is requested during switch reboots, power cycles, CP failovers, firmware downloads, and fabric reconfiguration.

If the user does not assign the insistent domain ID, the channel fails the query for security attributes and the channel does not come online. This parameter is for required for use with FICON only.

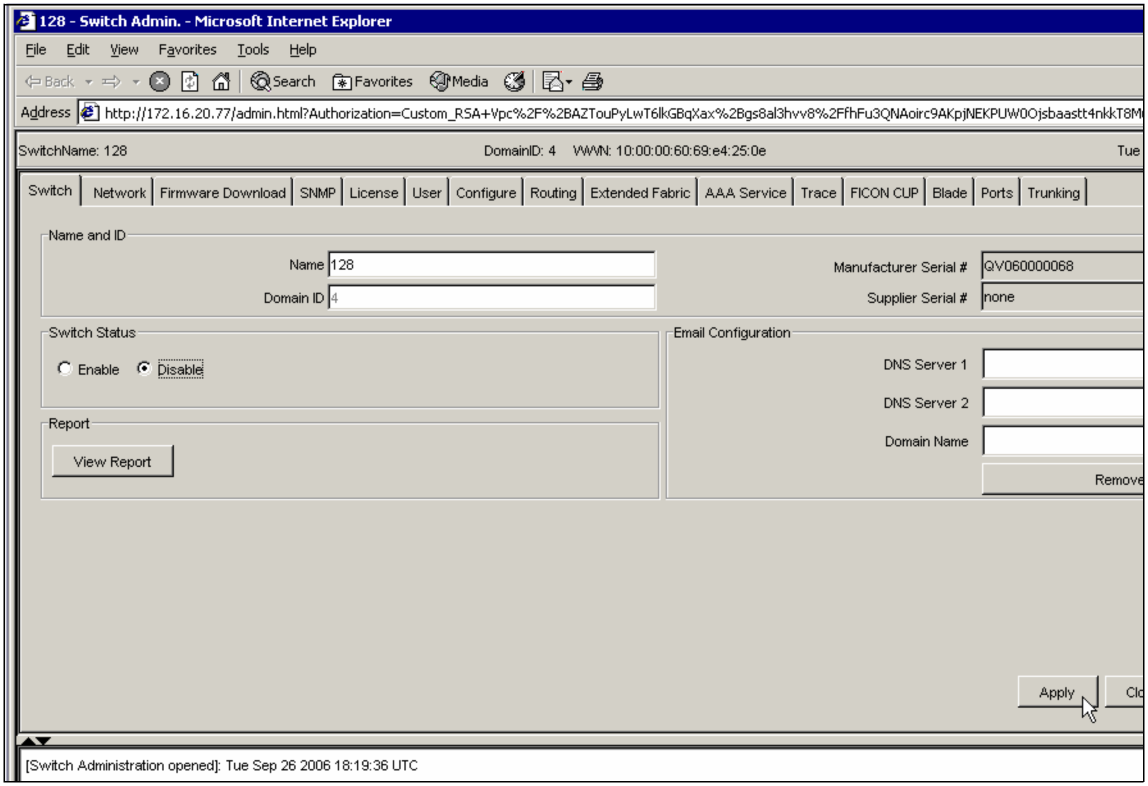
The Query Security Attributes (QSA) exchange is used by the host to determine that the fabric meets the above requirements.

> **Note:** A QSA is an ELS (extended link service) that a FICON host sends to determine fabric integrity. QSA is a snapshot of the fabric at login time; the host discovers changes in security attributes at next login. A QSA is issued when the channel is configured for 2-byte addressing; the IDID and Fabric binding bits must be set. If they are not, the channel does not enable the vary online if QSA returns false.

To set a unique domain ID and enable IDID mode, we complete the following steps:

1. Connect to the switch and log in as admin.
2. Disable the switch.
3. Verify that the switch has a unique domain ID. If it does not, set a unique domain ID.
4. Go to the **Switch** tab and configure a unique domain id.
5. Go to the **Configure** tab and enable Insistent Domain ID Mode.
6. Enable the switch.

We disable the switch as shown in Figure 1-278.


128 - Switch Admin. - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Switch Network Firmware Download SNMP License User Configure Routing Extended Fabric AAA Service Trace FICON CUP Blade Ports Trunking
Name and ID
Switch Status
Report
View Report
Email Configuration
DNS Server 1
DNS Server 2
Domain Name
Remove
Apply

http://172.16.20.77/admin.html?Authorization=Custom_RSA+Vpc%2F%2BAZTouPyLwT6lkGBqXax%2Bgs8al3hvv8%2FfhFu3QNAoirc9AKpjNEKPUW0Ojsbaastt4nkkT8M

SwitchName: 128 DomainID: 4 WWN: 10:00:00:60:69:e4:25:0e Tue

Name 128

Domain ID 4

Manufacturer Serial # QV060000068

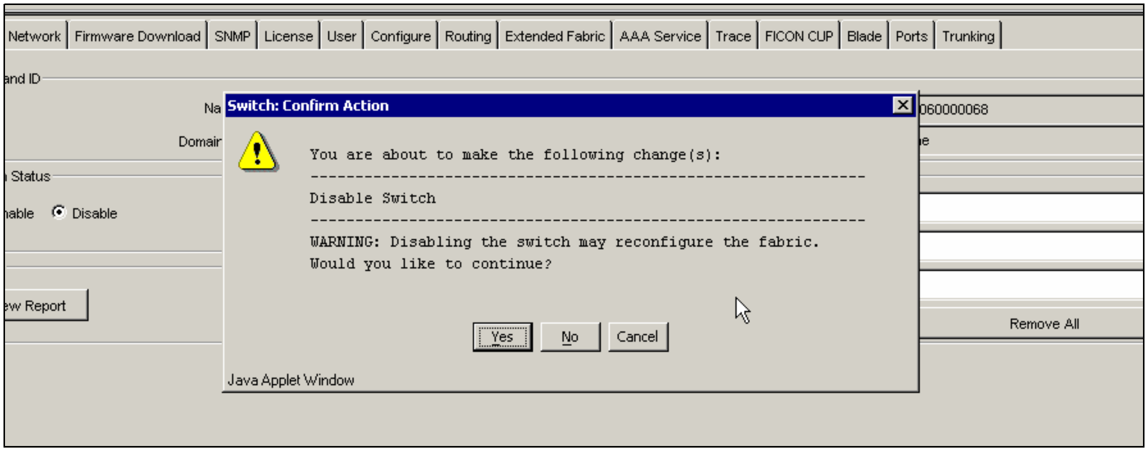
Supplier Serial # none

○ Enable ● Disable

[Switch Administration opened]: Tue Sep 26 2006 18:19:36 UTC

Figure 1-278 Disable switch

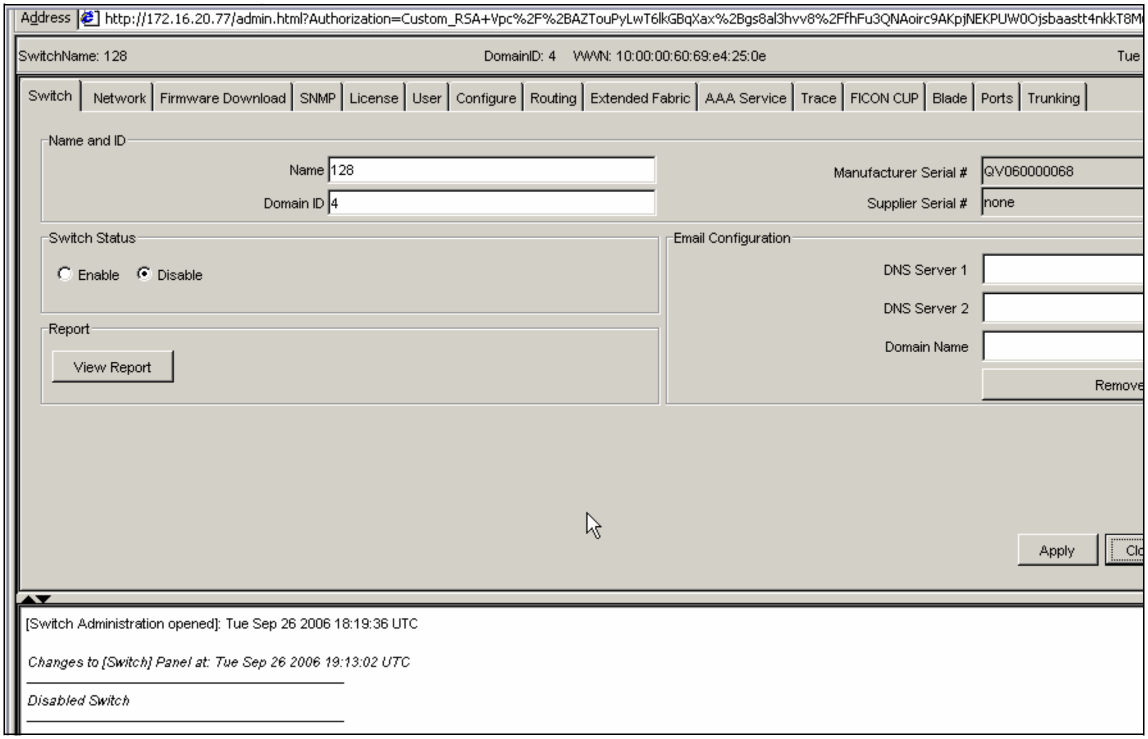
We confirm our action by clicking **Yes** as shown in Figure 1-279.


Network Firmware Download SNMP License User Configure Routing Extended Fabric AAA Service Trace FICON CUP Blade Ports Trunking
Switch: Confirm Action
Yes
No
Cancel
Java Applet Window
Remove All

```
You are about to make the following change(s):
------------------------------------------------------------
Disable Switch
------------------------------------------------------------
WARNING: Disabling the switch may reconfigure the fabric.
Would you like to continue?
```

Figure 1-279 Confirm disable

We verify the switch has a unique domain id (4 in our case) as shown in Figure 1-280.



Address http://172.16.20.77/admin.html?Authorization=Custom_RSA+Vpc%2F%2BAZTouPyLwT6lkGBqXax%2Bgs8al3hvv8%2FfhFu3QNAoirc9AKpjNEKPUW0Ojsbaastt4nkkT8M

SwitchName: 128

DomainID: 4

WWN: 10:00:00:60:69:e4:25:0e

Name: 128

Domain ID: 4

Manufacturer Serial #: QV060000068

Supplier Serial #: none

Switch Status: ○ Enable ● Disable

DNS Server 1:

DNS Server 2:

Domain Name:

[Switch Administration opened]: Tue Sep 26 2006 18:19:36 UTC

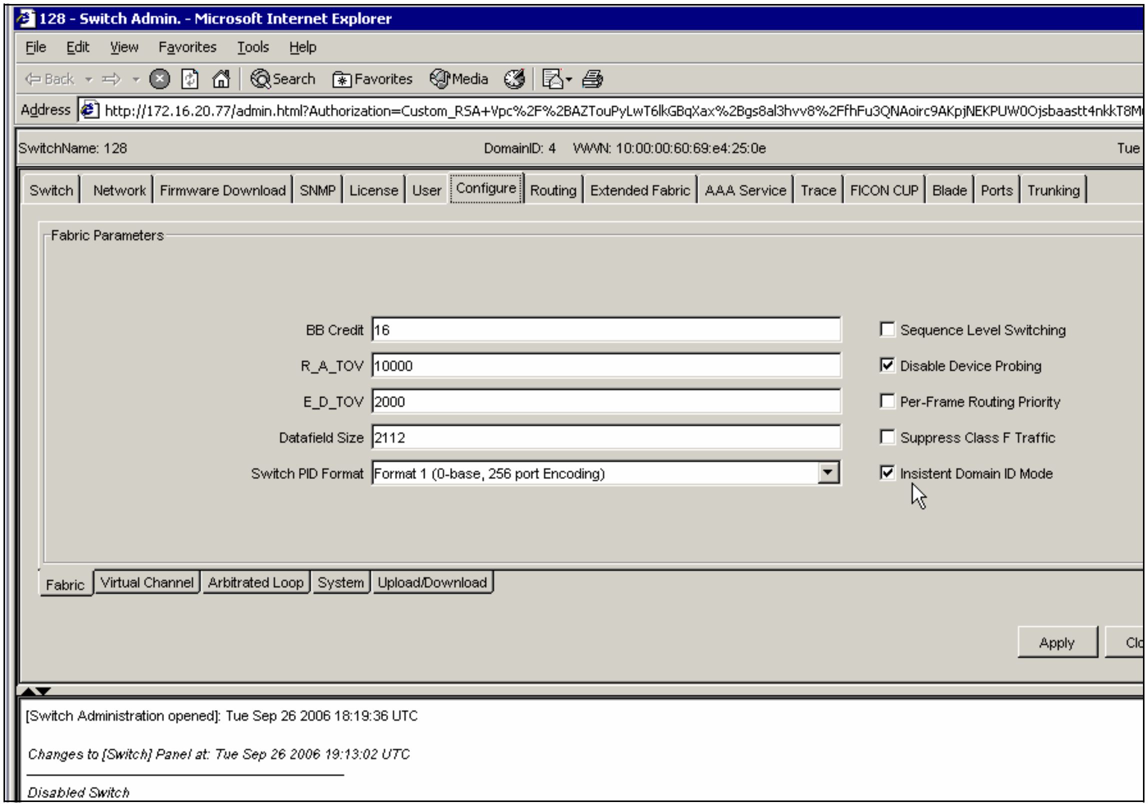
Changes to [Switch] Panel at: Tue Sep 26 2006 19:13:02 UTC

Disabled Switch

Tue
Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Blade
Ports
Trunking
Name and ID
Switch Status
Email Configuration
Report
View Report
Remove
Apply
Clo

Figure 1-280   Domain id

We then click the **Routing** tab to enable IDID mode as shown in Figure 1-281.


128 - Switch Admin. - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Switch Network Firmware Download SNMP License User Configure Routing Extended Fabric AAA Service Trace FICON CUP Blade Ports Trunking
Fabric Parameters
Fabric Virtual Channel Arbitrated Loop System Upload/Download
Apply
Clo

Address http://172.16.20.77/admin.html?Authorization=Custom_RSA+Vpc%2F%2BAZTouPyLwT6lkGBqXax%2Bgs8al3hvv8%2FfhFu3QNAoirc9AKpjNEKPUW0Ojsbaastt4nkkT8M

SwitchName: 128 DomainID: 4 WWN: 10:00:00:60:69:e4:25:0e Tue

BB Credit 16

R_A_TOV 10000

E_D_TOV 2000

Datafield Size 2112

Switch PID Format Format 1 (0-base, 256 port Encoding)

☐ Sequence Level Switching

☑ Disable Device Probing

☐ Per-Frame Routing Priority

☐ Suppress Class F Traffic

☑ Insistent Domain ID Mode

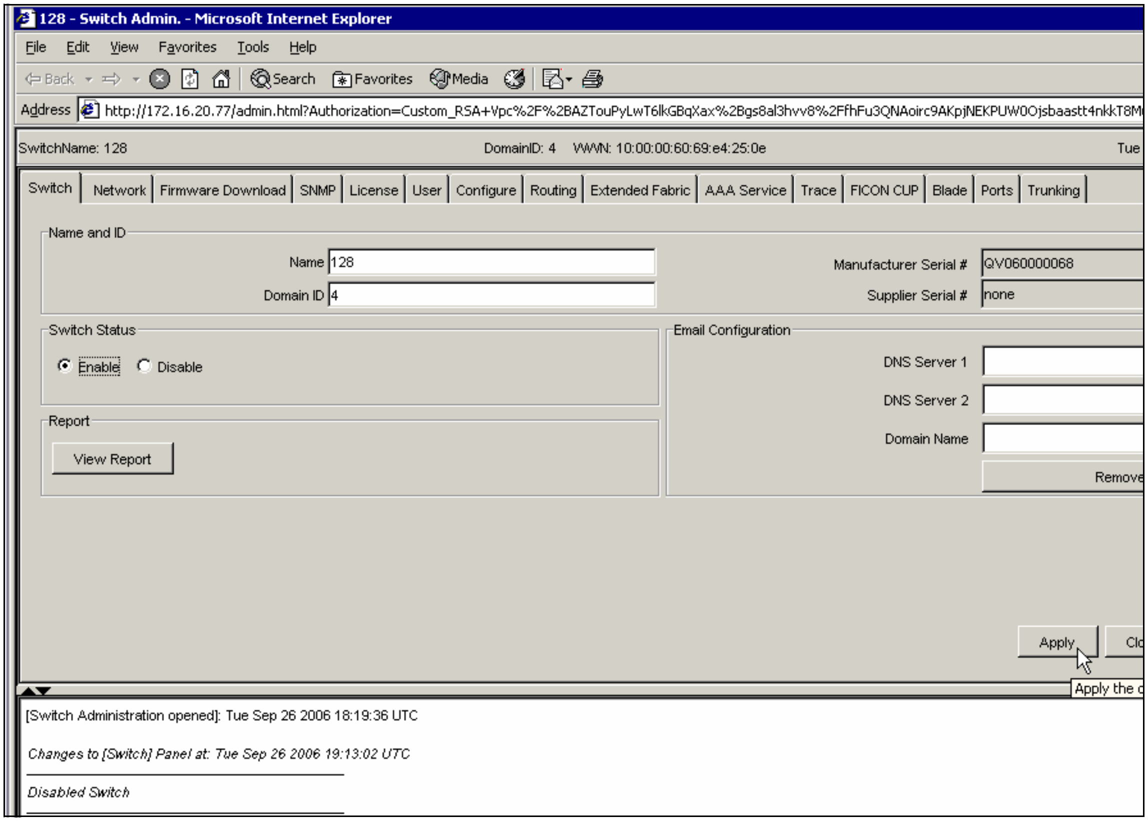
[Switch Administration opened]: Tue Sep 26 2006 18:19:36 UTC

Changes to [Switch] Panel at: Tue Sep 26 2006 19:13:02 UTC

Disabled Switch

Figure 1-281 IDID mode

We then enable the switch as shown in Figure 1-282.



128 - Switch Admin. - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Address
Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Blade
Ports
Trunking
Name and ID
Email Configuration
DNS Server 1
DNS Server 2
Domain Name
Remove
Report
View Report
Apply
Clo
Apply the c

http://172.16.20.77/admin.html?Authorization=Custom_RSA+Vpc%2F%2BAZTouPyLwT6lkGBqXax%2Bgs8al3hvv8%2FfhFu3QNAoirc9AKpjNEKPUW0Ojsbaastt4nkkT8M

SwitchName: 128 DomainID: 4 WWN: 10:00:00:60:69:e4:25:0e Tue

Name 128

Domain ID 4

Manufacturer Serial # QV060000068

Supplier Serial # none

Switch Status

● Enable ○ Disable

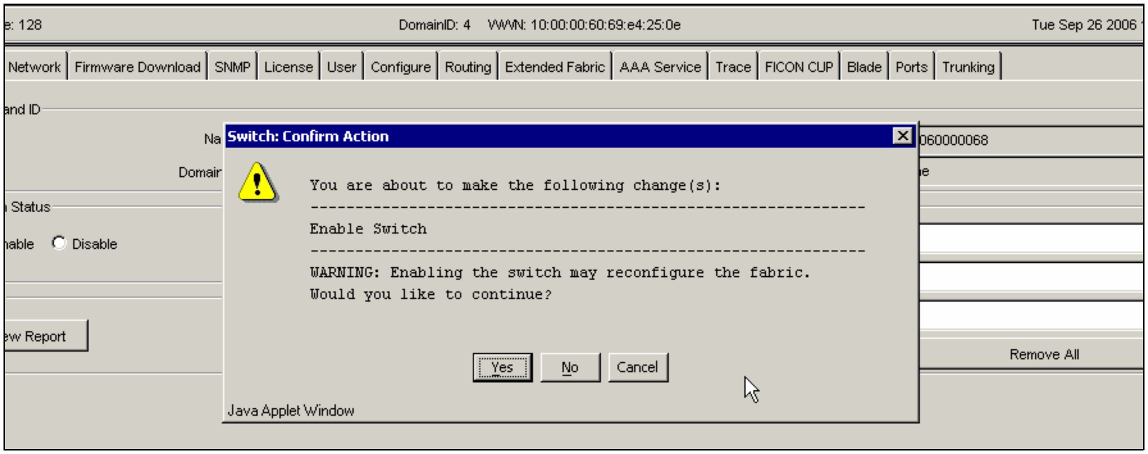
[Switch Administration opened]: Tue Sep 26 2006 18:19:36 UTC

Changes to [Switch] Panel at: Tue Sep 26 2006 19:13:02 UTC

Disabled Switch

Figure 1-282 Enable switch

We confirm that we want to enable the switch by clicking **Yes** as shown in Figure 1-283.


e: 128
DomainID: 4 WWN: 10:00:00:60:69:e4:25:0e
Tue Sep 26 2006
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Blade
Ports
Trunking
and ID
Na
Domain
Status
able
Disable
w Report
060000068
Remove All
Switch: Confirm Action
Yes
No
Cancel
Java Applet Window

```
You are about to make the following change(s):
--------------------------------------------------------------
Enable Switch
--------------------------------------------------------------
WARNING: Enabling the switch may reconfigure the fabric.
Would you like to continue?
```

Figure 1-283 Confirm enable

We have now set a unique domain id and set insistent domain id mode.

Note: Both of these must be set on a per switch basis.

1.14 Preparing a cascaded FICON configuration

Setting the unique domain id and insistent domain id are two necessary steps in preparing for a cascaded FICON environment. We describe the security tasks that have to be taken to support the cascaded environment in the topics that follow.

1.14.1 Installing security certificates and keys

Secure Fabric OS requires that each switch in the fabric has PKI objects and a digital certificate. To verify whether the objects and a digital certificate are correctly installed in the fabric, login to one of the switches in the fabric as admin, and issue the **`pkishow`** command as shown in Example 1-52.

Example 1-52 pkishow command

```
128:admin> pkishow
Passphrase      : Exist
Private Key     : Exist
CSR             : Exist
Certificate     : Exist
Root Certificate: Exist
```

As can be seen, we already have the certificates and objects installed.

To install the certificates and keys, refer to 1.9.8, “Advanced Security” on page 274 for details. Although that process is for a different switch, the process is the same.

Attention: For FICON cascading you must install Secure Fabric OS and PKI certificates on all switches in the fabric.

1.14.2 Enabling secure mode

Secure mode is enabled and disabled on a fabric-wide basis. Secure mode can be enabled and disabled as often as desired; however, all Secure Fabric OS policies, including the FCS policy, are deleted each time secure mode is disabled, and they must be re-created the next time it is enabled.

Secure mode is enabled using the **`secModeEnable`** command as shown in Example 1-53. This command must be entered through a sectelnet, SSH, or serial connection to the switch designated as the primary FCS switch. The command fails if any switch in the fabric is not capable of enforcing Secure Fabric OS policies. If the primary FCS switch fails to participate in the fabric, the role of the primary FCS switch moves to the next available switch listed in the FCS policy.

Example 1-53 secmodenable command

```
128:admin> secmodeenable --lockdown=scc --currentpwd --fcs "*"
Your use of the certificate-based security features of the software
installed on this equipment is subject to the End User License Agreement
provided with the equipment and the Certification Practices Statement,
which you may review at http://www.switchkeyactivation.com/cps. By using
these security features, you are consenting to be bound by the terms of
these documents. If you do not agree to the terms of these documents,
promptly contact the entity from which you obtained this software and do
not use these security features.
Do you agree to these terms? (yes, y, no, n): [no] y
This command requires Switch Certificate, Security license and Zoning license
to be installed on every switch in the fabric.
PLEASE NOTE: On successful completion of this command, login sessions may be
closed and some switches may go through a reboot to form a secure fabric.
Non-FCS admin password will be set the same as FCS admin password.
ARE YOU SURE (yes, y, no, n): [no] y
Please enter current admin account password:
Enabling secure mode, this may take several minutes, please wait...
Secure mode is enabled.
128:admin>
```

We confirm that secure mode is enabled, and that our switches are included by issuing a series of commands. These are shown in Example 1-54.

Example 1-54 secmodeshow, secpolicyshow and secfabricshow

```
128:admin> secmodeshow
Secure Mode: ENABLED.
Version Stamp: 852064845, Fri Aug  4 15:42:14 2006.
Pos   Primary WWN                     DId swName.
=================================================
  1   Yes     10:00:00:60:69:e4:25:12   5 M48
  2   No      10:00:00:60:69:e4:25:0e   4 128
128:admin>

128:admin> secpolicyshow


____________________________________________________
                ACTIVE POLICY SET
FCS_POLICY
   Pos   Primary WWN                     DId swName
   __________________________________________________
     1   Yes     10:00:00:60:69:e4:25:12   5 M48
     2   No      10:00:00:60:69:e4:25:0e   4 128

SCC_POLICY
   WWN                     DId swName
   __________________________________________________
   10:00:00:60:69:e4:25:12   5
   10:00:00:60:69:e4:25:0e   4 128

                DEFINED POLICY SET
FCS_POLICY
   Pos   Primary WWN                     DId swN
   _____________________________________________
     1   Yes     10:00:00:60:69:e4:25:12   5 M48
     2   No      10:00:00:60:69:e4:25:0e   4 128

SCC_POLICY
   WWN                     DId swName
   _____________________________________________
   10:00:00:60:69:e4:25:12   5 M48
   10:00:00:60:69:e4:25:0e   4 128

128:admin> secfabricshow
Role    WWN                     DId Status  Enet IP Addr    Name
================================================================
Backup  10:00:00:60:69:e4:25:0e   4 Ready   172.16.20.77    "128"
Primary 10:00:00:60:69:e4:25:12   5 Ready   172.16.20.74    "M48"
```

```
Secured switches in the fabric: 2
```

1.14.3 Configuring Switch Connection Control

The Switch Connection Control (SCC) policy is used to restrict which switches can join the fabric, also known as fabric binding. Switches are checked against the policy each time secure mode is enabled, the fabric is initialized with secure mode enabled, or an E_Port-to-E_Port connection is made. The policy is named SCC_POLICY and accepts members listed as WWNs, domain IDs, or switch names. Only one SCC policy can be created. By default, any switch is allowed to join the fabric; the SCC policy does not exist until it is created by the administrator.

The SCC policy defines all switches in the secure fabric (FCS and non-FCS). You cannot add a new switch to a secure fabric without adding the switch to the SCC policy. You cannot add a switch to the SCC policy until you create an SCC policy. SCC policies are created automatically in Fabric Manager when you enable secure mode on a fabric.

To configure/edit the SCC policy, right-click the primary FCS switch of the secure fabric that you want to set policies on from within the SAN Elements tab and select **Security** →**Security Policy Editor** from the context menu, as shown in Figure 1-284.

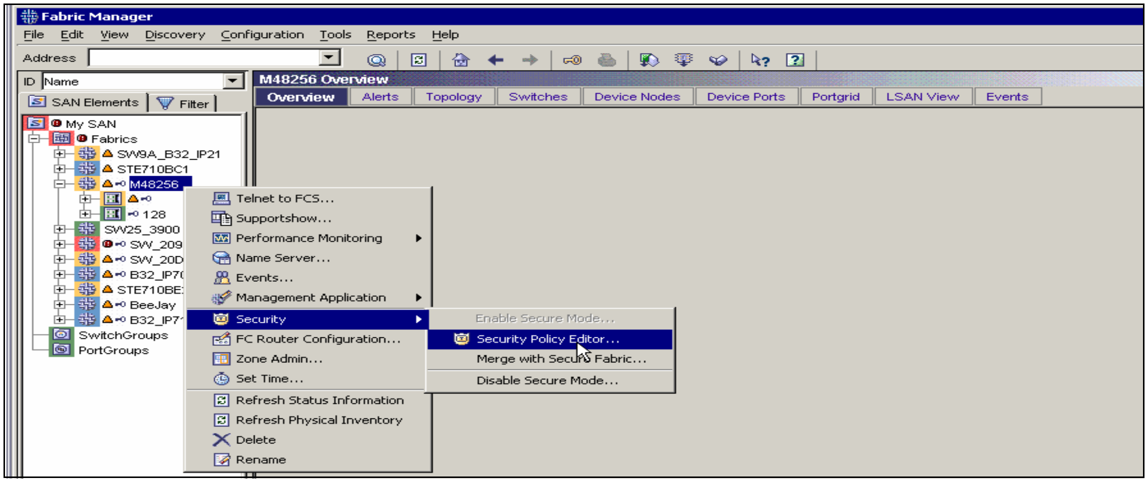
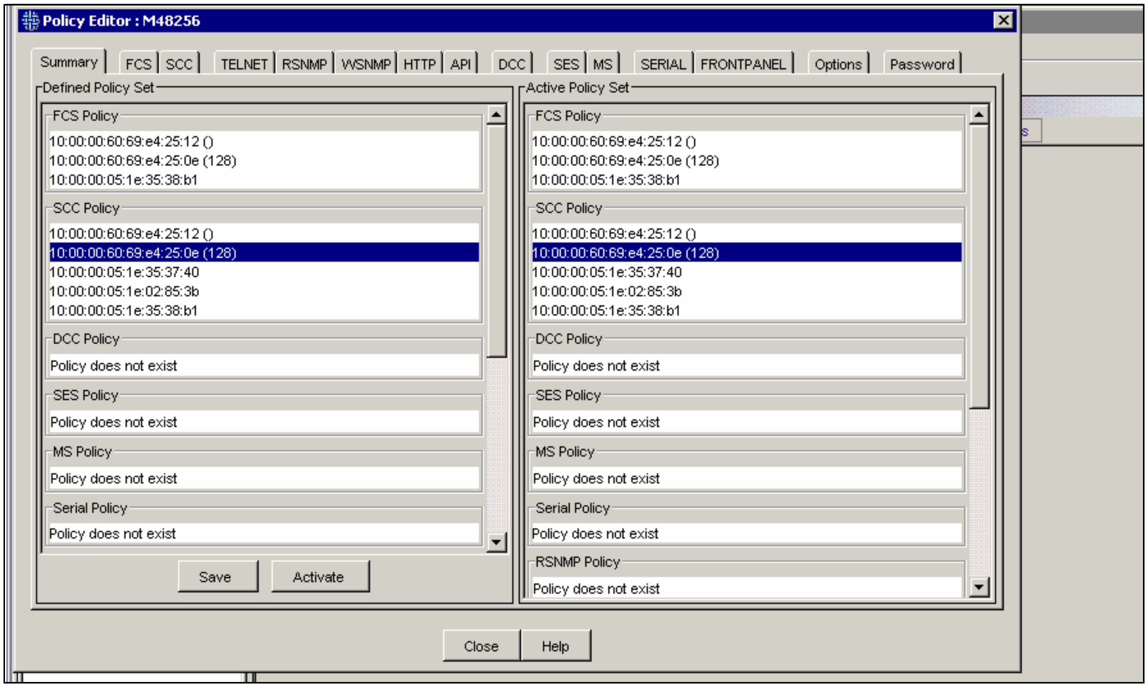

Fabric Manager
File
Edit
View
Discovery
Configuration
Tools
Reports
Help
Address
ID
Name
SAN Elements
Filter
M48256 Overview
Overview
Alerts
Topology
Switches
Device Nodes
Device Ports
Portgrid
LSAN View
Events
My SAN
Fabrics
SW9A_B32_IP21
STE710BC1
M48256
128
SW25_3900
SW_209
SW_20D
B32_IP7(
STE710BE
BeeJay
B32_IP7
SwitchGroups
PortGroups
Telnet to FCS...
Supportshow...
Performance Monitoring
Name Server...
Events...
Management Application
Security
FC Router Configuration...
Zone Admin...
Set Time...
Refresh Status Information
Refresh Physical Inventory
Delete
Rename
Enable Secure Mode...
Security Policy Editor...
Merge with Secure Fabric...
Disable Secure Mode...

Figure 1-284 Security policy editor

The Policy Editor appears as shown in Figure 1-285.


Policy Editor : M48256
Summary
FCS
SCC
TELNET
RSNMP
WSNMP
HTTP
API
DCC
SES
MS
SERIAL
FRONTPANEL
Options
Password
Save
Activate
Close
Help

Defined Policy Set

FCS Policy
10:00:00:60:69:e4:25:12 ()
10:00:00:60:69:e4:25:0e (128)
10:00:00:05:1e:35:38:b1

SCC Policy
10:00:00:60:69:e4:25:12 ()
10:00:00:60:69:e4:25:0e (128)
10:00:00:05:1e:35:37:40
10:00:00:05:1e:02:85:3b
10:00:00:05:1e:35:38:b1

DCC Policy
Policy does not exist

SES Policy
Policy does not exist

MS Policy
Policy does not exist

Serial Policy
Policy does not exist

Active Policy Set

FCS Policy
10:00:00:60:69:e4:25:12 ()
10:00:00:60:69:e4:25:0e (128)
10:00:00:05:1e:35:38:b1

SCC Policy
10:00:00:60:69:e4:25:12 ()
10:00:00:60:69:e4:25:0e (128)
10:00:00:05:1e:35:37:40
10:00:00:05:1e:02:85:3b
10:00:00:05:1e:35:38:b1

DCC Policy
Policy does not exist

SES Policy
Policy does not exist

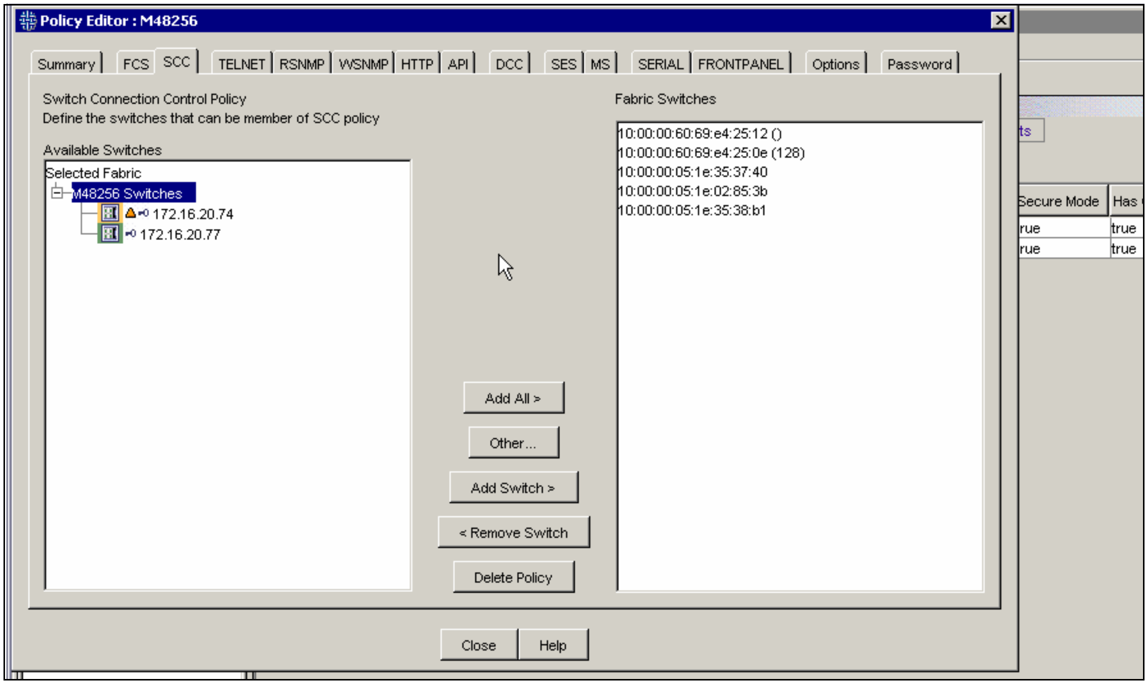
MS Policy
Policy does not exist

Serial Policy
Policy does not exist

RSNMP Policy
Policy does not exist

Figure 1-285 Summary

We click the **SCC** tab. All current switches in the fabric display in the Available Switches list as shown in Figure 1-286.


Policy Editor : M48256
Summary
FCS
SCC
TELNET
RSNMP
WSNMP
HTTP
API
DCC
SES
MS
SERIAL
FRONTPANEL
Options
Password
Add All >
Other...
Add Switch >
< Remove Switch
Delete Policy
Close
Help
ts
Secure Mode
Has

Switch Connection Control Policy

Define the switches that can be member of SCC policy

Available Switches

Selected Fabric
- M48256 Switches
  - 172.16.20.74
  - 172.16.20.77

Fabric Switches

```
10:00:00:60:69:e4:25:12 ()
10:00:00:60:69:e4:25:0e (128)
10:00:00:05:1e:35:37:40
10:00:00:05:1e:02:85:3b
10:00:00:05:1e:35:38:b1
```

Secure Mode	Has
rue	true
rue	true

Figure 1-286 SCC switches

Click a switch that you want to include in the SCC policy and click Add Switch, or click Add All to add all switches from the fabric into the policy.

To add a switch that is not listed in the Available Switch list, click Other, and type the WWN of the switch you want to add.

1.14.4 Enabling FICON CUP

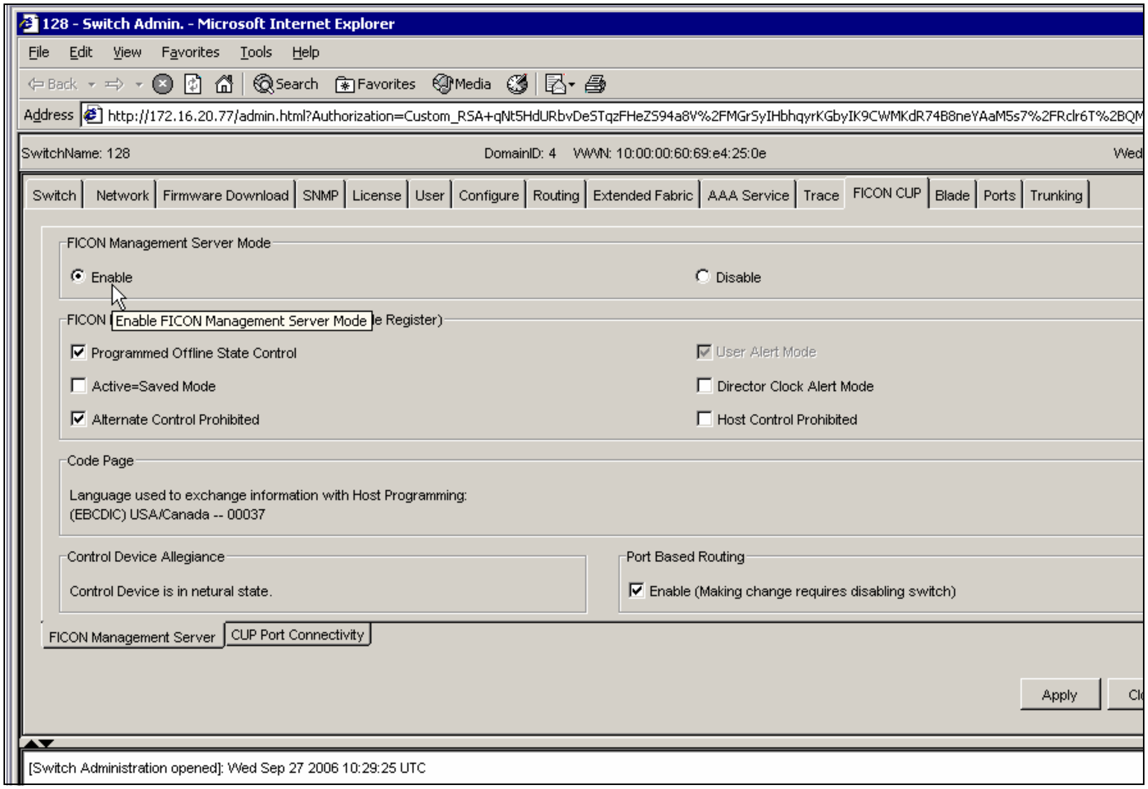
Host-based management programs manage switches using CUP protocol by sending commands to an emulated control device in Fabric OS. A switch that supports CUP can be controlled by one or more host-based management programs, as well as by Web Tools. A mode register controls the behavior of the switch with respect to CUP itself, and with respect to the behavior of other management interfaces.

The FICON CUP license must be installed, FICON Management Server (FMS) mode must be enabled, and the configure CUP attributes (FMS parameters) for the FICON director on the switch set to enable CUP management features.

Enabling FMS mode

When FMS mode is enabled, Fabric OS prevents local switch commands from interfering with host-based management commands by initiating serialized access to switch parameters. If more than one switch is to be used in the FICON CUP fabric, Secure Fabric OS *must* be installed.

To enable FMS mode from the FICON CUP tab check the FICON Management Server Mode Enable button as shown in Figure 1-287.


128 - Switch Admin. - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Switch Network Firmware Download SNMP License User Configure Routing Extended Fabric AAA Service Trace FICON CUP Blade Ports Trunking
FICON Management Server
CUP Port Connectivity
Apply
Enable FICON Management Server Mode

http://172.16.20.77/admin.html?Authorization=Custom_RSA+qNt5HdURbvDeSTqzFHeZS94a8V%2FMGrSyIHbhqyrKGbyIK9CWMKdR74B8neYAaM5s7%2FRclr6T%2BQM

SwitchName: 128 DomainID: 4 WWN: 10:00:00:60:69:e4:25:0e

FICON Management Server Mode

● Enable ○ Disable

FICON (Control Unit Port) Register)

☑ Programmed Offline State Control
☐ Active=Saved Mode
☑ Alternate Control Prohibited
☑ User Alert Mode
☐ Director Clock Alert Mode
☐ Host Control Prohibited

Code Page

Language used to exchange information with Host Programming:
(EBCDIC) USA/Canada -- 00037

Control Device Allegiance

Control Device is in netural state.

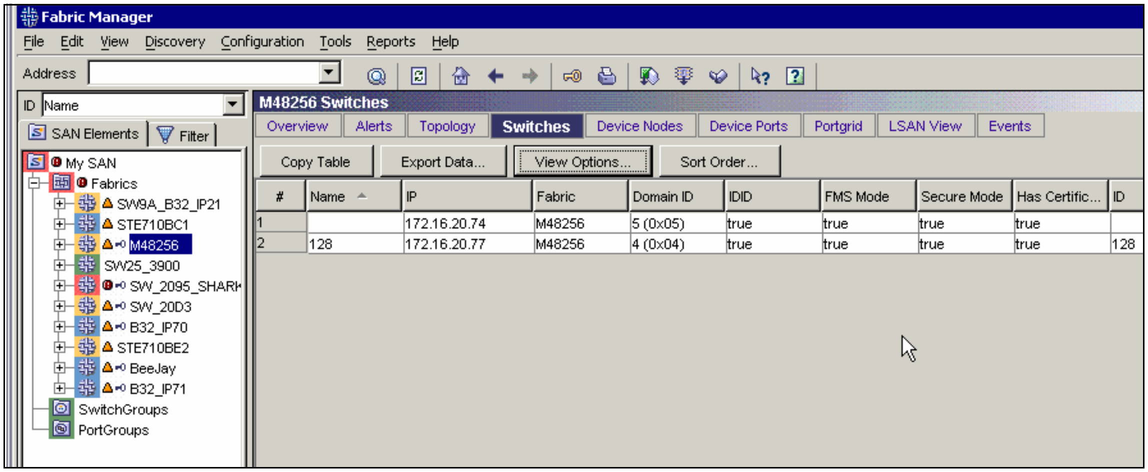
Port Based Routing

☑ Enable (Making change requires disabling switch)

[Switch Administration opened]: Wed Sep 27 2006 10:29:25 UTC

Figure 1-287 FMS mode

To verify that FMS mode is set we select the fabric (M48256) and click the **Switches** view. From the resultant display we can see that FMS mode is set for the switches in our fabric as in Figure 1-288.


Fabric Manager
File Edit View Discovery Configuration Tools Reports Help
Address
ID Name
SAN Elements
Filter
My SAN
Fabrics
SW9A_B32_IP21
STE710BC1
M48256
SW25_3900
SW_2095_SHARK
SW_20D3
B32_IP70
STE710BE2
BeeJay
B32_IP71
SwitchGroups
PortGroups
M48256 Switches
Overview
Alerts
Topology
Switches
Device Nodes
Device Ports
Portgrid
LSAN View
Events
Copy Table
Export Data...
View Options...
Sort Order...

#	Name	IP	Fabric	Domain ID	IDID	FMS Mode	Secure Mode	Has Certific...	ID
1		172.16.20.74	M48256	5 (0x05)	true	true	true	true	
2	128	172.16.20.77	M48256	4 (0x04)	true	true	true	true	128

Figure 1-288 FMS mode true

Enabling FMS parameters

FMS parameters control the behavior of the switch with respect to CUP itself, as well as the behavior of other management interfaces (director console, Alternate Managers). You can configure FMS parameters for a switch only after FMS mode is enabled on the switch. All FMS parameter settings are persistent across switch power cycles. There are six FMS parameters:

- Programmed Offline State Control:

  This parameter controls whether host programming is allowed to set the switch offline. The parameter is set as enabled by the hardware after system installation, and can be reset by Web Tools.

- Active=Saved Mode:

  This parameter controls the IPL file update. The IPL file saves port connectivity attributes and port names. After a switch reboot or power cycle, the switch reads the IPL file and actives its contents as default configuration.

  When this mode is enabled, activating a configuration saves a copy to the IPL configuration file. All changes made to the active connectivity attributes or port names by host programming or alternate managers are saved in this IPL file. It keeps the current active configuration persistent across switch reboots and power cycles. You cannot directly modify the IPL file or save a file as an IPL file. When this mode is disabled, the IPL file is not altered for either new configuration activation or any changes made on the current active configuration. This parameter is set as enabled by the hardware after system installation, and can be reset by Web Tools.

Note: When FMS mode is enabled and the Active=Saved parameter is disabled, you can enable and disable ports, but the setting is not persistent. When the Active=Saved parameter is enabled, you can enable and disable ports and the setting is persistent.

- Alternate Control Prohibited:

  This parameter determines whether alternate managers are allowed to modify port connectivity. Enabling this mode prohibits alternate manager control of port connectivity; otherwise, alternate managers can manage port connectivity. This parameter is set as enabled by the hardware after system installation, and can be reset by Web Tools.

- User Alert Mode:

  This parameter controls director console behavior for alerts. Enabling this mode prompts the director consoles to display a warning whenever you attempt an action that will change switch parameters. When you disable this mode, no warning is displayed. In this case, in which Web Tools is the director console, warning messages are displayed by Web Tools regardless of the setting of the parameter, since Web Tools always displays warning messages when you apply a change to a switch that changes parameters. This parameter is always read-only in Web Tools. Each time that the switch is powered on, the parameter is reset to disabled.

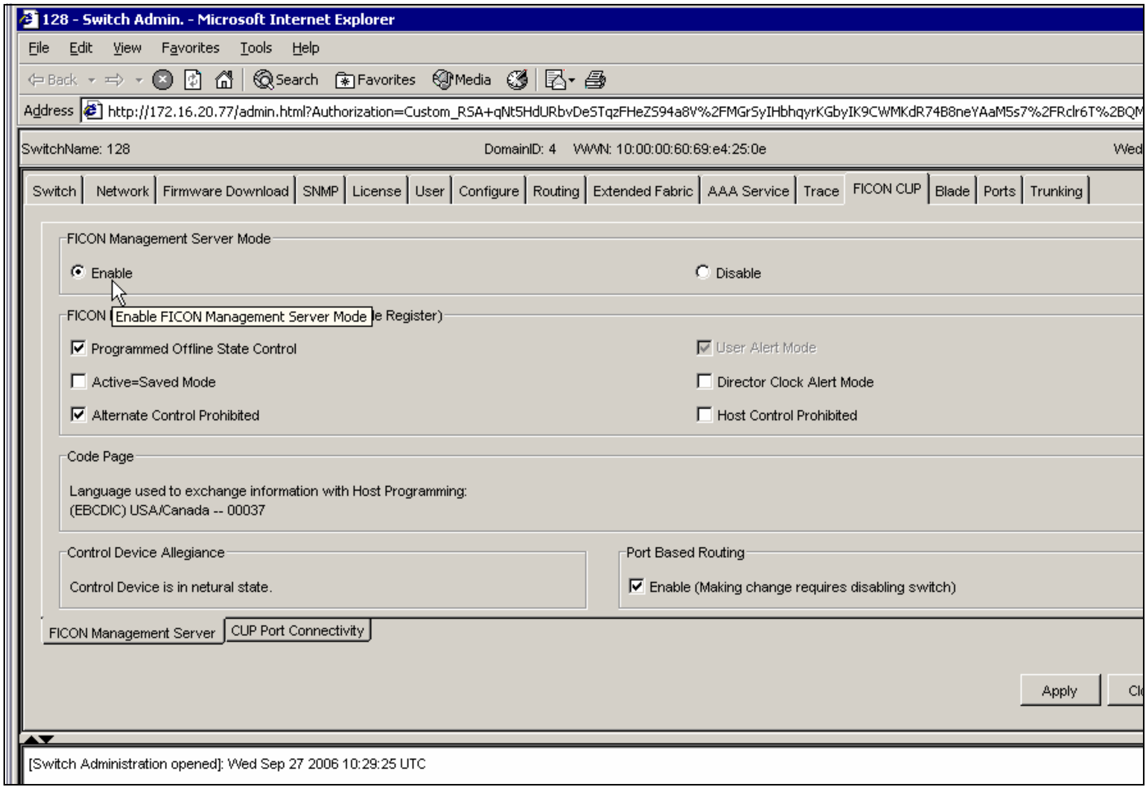
- Director Clock Alert Mode:

  This parameter controls behavior for attempts to set the switch timestamp clock through the director console. When it is enabled, the director console (Web Tools, in this case) displays warning indications when the switch timestamp is changed by a user application. When it is disabled, you can activate a function to automatically set the timestamp clock. There is no indication for timestamp clock setting. This parameter is set as disabled by the hardware after system installation, and can be reset by Web Tools.

- Host Control Prohibited:

  This parameter determines whether host programming allows modifying port connectivity. Enabling this mode prohibits host programming control of port connectivity; otherwise, host programming can manage port connectivity. This parameter is set as disabled by the hardware after system installation. and can be reset by Web Tools.

Setting the FMS parameters is performed on the same screen that we enabled FMS mode, as shown in Figure 1-289.


128 - Switch Admin. - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://172.16.20.77/admin.html?Authorization=Custom_RSA+qNt5HdURbvDeSTqzFHeZ594a8V%2FMGrSyIHbhqyrKGbyIK9CWMKdR74B8neYAaM5s7%2FRclr6T%2BQM
Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Blade
Ports
Trunking
Enable FICON Management Server Mode
FICON Management Server
CUP Port Connectivity
Apply
Cl

SwitchName: 128 DomainID: 4 WWN: 10:00:00:60:69:e4:25:0e Wed

FICON Management Server Mode

● Enable ○ Disable

FICON (... e Register)

☑ Programmed Offline State Control

☑ User Alert Mode

☐ Active=Saved Mode

☐ Director Clock Alert Mode

☑ Alternate Control Prohibited

☐ Host Control Prohibited

Code Page

Language used to exchange information with Host Programming:
(EBCDIC) USA/Canada -- 00037

Control Device Allegiance

Control Device is in netural state.

Port Based Routing

☑ Enable (Making change requires disabling switch)

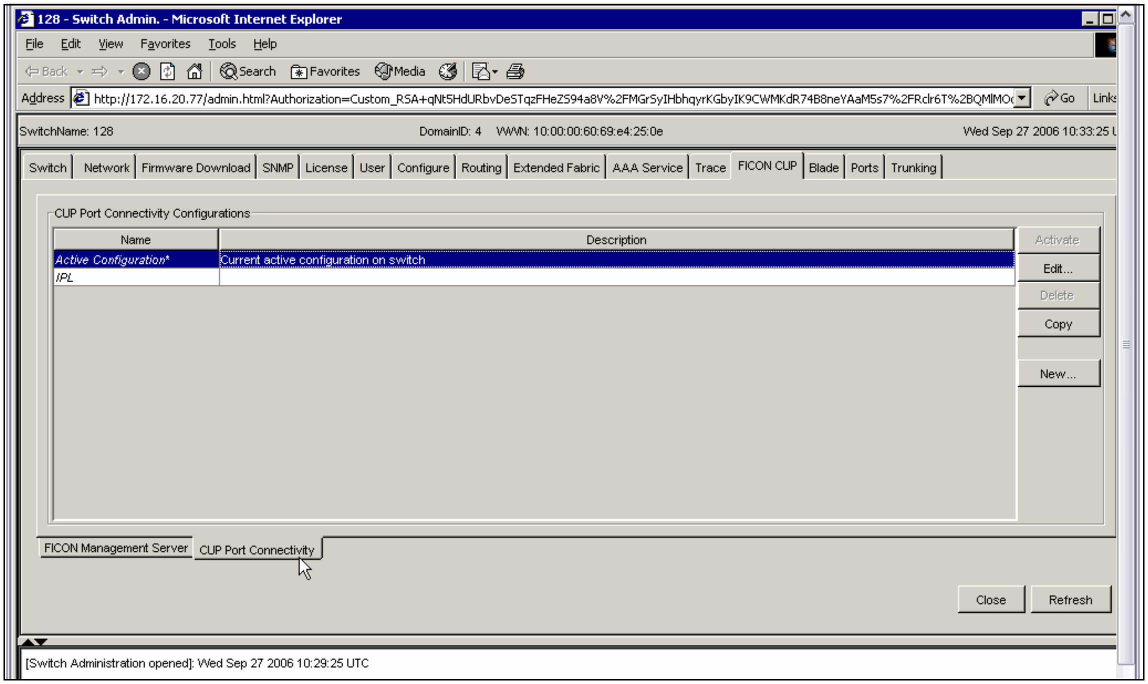
[Switch Administration opened]: Wed Sep 27 2006 10:29:25 UTC

Figure 1-289 FMS parameters

1.14.5 Configuring port connectivity

The Port Dynamic Connectivity Mask (PDCM) is a mechanism to define port connectivity (also referred to as prohibit/allow).

In the Port Connectivity subpanel (shown in Figure 1-290), you can manage the configuration files and active configuration. All CUP configuration files and the active configuration are listed in a table. The active configuration is listed as “Active Configuration*” and the description in the table is “Current active configuration on switch.” The other special configuration file is the IPL. Any other files displayed are user-defined configurations and are stored on the switch.


128 - Switch Admin. - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Links
Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Blade
Ports
Trunking
CUP Port Connectivity Configurations
Activate
Edit...
Delete
Copy
New...
FICON Management Server
CUP Port Connectivity
Close
Refresh

http://172.16.20.77/admin.html?Authorization=Custom_RSA+qNt5HdURbvDeSTqzFHeZS94a8V%2FMGrSyIHbhqyrKGbyIK9CWMKdR74B8neYAaM5s7%2FRclr6T%2BQMlMO

SwitchName: 128 DomainID: 4 WWN: 10:00:00:60:69:e4:25:0e Wed Sep 27 2006 10:33:25

Name	Description
*Active Configuration**	Current active configuration on switch
IPL	

[Switch Administration opened]: Wed Sep 27 2006 10:29:25 UTC

Figure 1-290 CUP port connectivity

You can create, activate, copy, or delete saved CUP port connectivity configurations; however, you can only edit or copy a configuration while it is active.

You can also activate, edit, or copy the IPL configuration. You *must* have FMS mode enabled before you can make any changes to the configurations. Click **Refresh** to get the latest configuration file list from the switch.

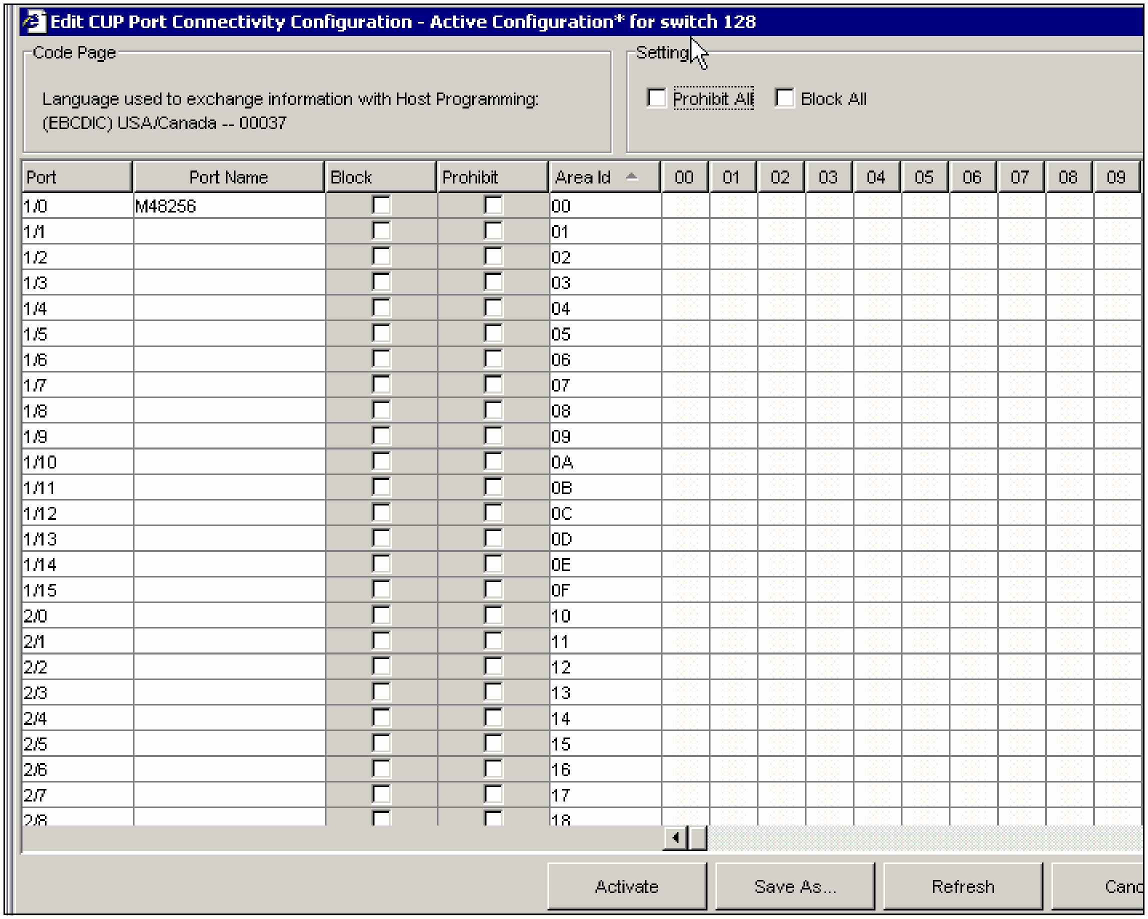
When creating a new configuration or editing an existing configuration, keep in mind that the Web Tools port name input is restricted to printable ASCII characters. Therefore, when Web Tools displays a port name, if there are characters beyond printable ASCII characters (which would have been created by the Host Program), those characters are displayed as dots (.).

When initially installed, a switch allows *any* port to dynamically communicate with any other port. Two connectivity attributes are defined to restrict this any-to-any capability for external ports: Block and Prohibit:

- Block is a port connectivity attribute that prevents all communication through a port.

- Prohibit is the port connectivity attribute that prohibits or allows dynamic communication between ports when a port is not blocked. Each port has a vector specifying its Prohibit attribute with respect to each of the other ports in the switch. This attribute is always set symmetrically in that a pair of ports is either prohibited or allowed to communicate dynamically.

The Port Connectivity table (shown in Figure 1-291) displays the Port number (in physical-location format), Port Name (port address name), Block attribute, Prohibit attribute, and Area ID (port address, displayed in hexadecimal) in fixed columns. The right side is a port matrix, which lists all ports by Area ID and identifies prohibited ports. Those columns are scrollable and swappable.



Edit CUP Port Connectivity Configuration - Active Configuration* for switch 128

Code Page

Language used to exchange information with Host Programming:
(EBCDIC) USA/Canada -- 00037

Setting

☐ Prohibit All ☐ Block All

Port	Port Name	Block	Prohibit	Area Id	00	01	02	03	04	05	06	07	08	09
1/0	M48256	☐	☐	00										
1/1		☐	☐	01										
1/2		☐	☐	02										
1/3		☐	☐	03										
1/4		☐	☐	04										
1/5		☐	☐	05										
1/6		☐	☐	06										
1/7		☐	☐	07										
1/8		☐	☐	08										
1/9		☐	☐	09										
1/10		☐	☐	0A										
1/11		☐	☐	0B										
1/12		☐	☐	0C										
1/13		☐	☐	0D										
1/14		☐	☐	0E										
1/15		☐	☐	0F										
2/0		☐	☐	10										
2/1		☐	☐	11										
2/2		☐	☐	12										
2/3		☐	☐	13										
2/4		☐	☐	14										
2/5		☐	☐	15										
2/6		☐	☐	16										
2/7		☐	☐	17										
2/8		☐	☐	18										

Figure 1-291 Port connectivity table

To create or edit CUP port connectivity configurations, display the CUP port connectivity configuration list as shown in Figure 1-291. In this case we have chosen to edit an existing configuration.

The Create Port CUP Connectivity Configuration dialog displays all ports and port names on the selected switch. The Block column, Prohibit column, and prohibited ports matrix are displayed as empty:

- **Optional**: Check the checkbox corresponding to a port you want to block on the Block column.

  Repeat this step for all ports you want to block. Click the Block All checkbox to block all ports.

- **Optional**: Check the checkbox corresponding to a port you want to prohibit on the Prohibit column.

  Repeat this step for all ports you want to prohibit. Click the Prohibit All checkbox to prohibit all ports.

  The cells in the matrix are updated with “X” icons to identify prohibited ports.

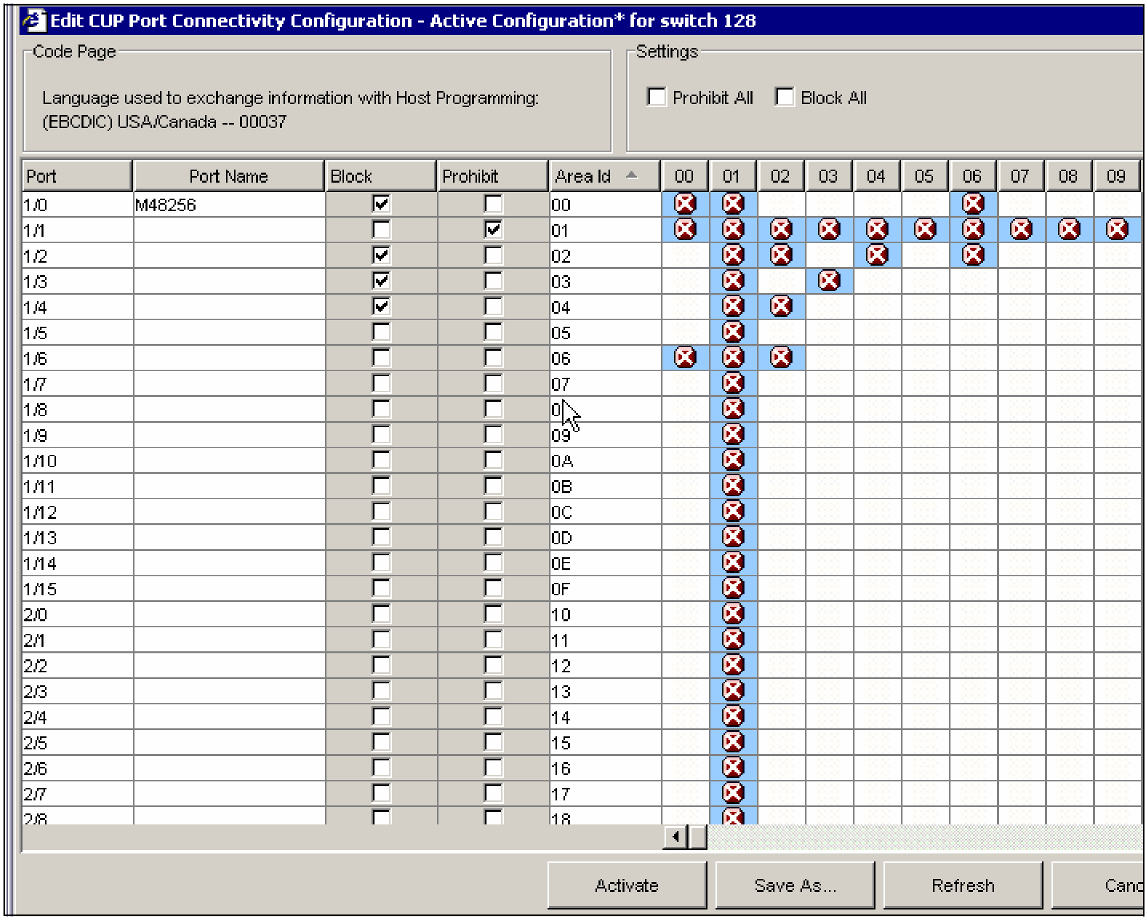
- **Optional**: Click the individual cells corresponding to the combination of ports you want to prohibit.

  You cannot prohibit a port to itself.

Review your changes. A blue background in a cell indicates that its value has been modified. After you have finished making changes, do any of the following actions:

- Click **Activate** to save the changes and make the configuration active immediately.
- Click **Save** to save the changes, but do not make the configuration active.
- Click **Save As** to save the configuration to a new configuration file. When you click **Save As**, a dialog displays allowing you to type a file name and description for the configuration file.
- Click **Refresh** to refresh the information from the switch.
- Click **Cancel** to cancel all changes without saving.

In Figure 1-292 we show the matrix with selections made.



Edit CUP Port Connectivity Configuration - Active Configuration* for switch 128

Code Page

Language used to exchange information with Host Programming: (EBCDIC) USA/Canada -- 00037

Settings

☐ Prohibit All ☐ Block All

Port	Port Name	Block	Prohibit	Area Id	00	01	02	03	04	05	06	07	08	09
1/0	M48256	☑	☐	00	☒	☒					☒			
1/1		☐	☑	01	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
1/2		☑	☐	02		☒	☒		☒		☒			
1/3		☑	☐	03		☒		☒						
1/4		☑	☐	04		☒	☒							
1/5		☐	☐	05		☒								
1/6		☐	☐	06	☒	☒	☒							
1/7		☐	☐	07		☒								
1/8		☐	☐	0		☒								
1/9		☐	☐	09		☒								
1/10		☐	☐	0A		☒								
1/11		☐	☐	0B		☒								
1/12		☐	☐	0C		☒								
1/13		☐	☐	0D		☒								
1/14		☐	☐	0E		☒								
1/15		☐	☐	0F		☒								
2/0		☐	☐	10		☒								
2/1		☐	☐	11		☒								
2/2		☐	☐	12		☒								
2/3		☐	☐	13		☒								
2/4		☐	☐	14		☒								
2/5		☐	☐	15		☒								
2/6		☐	☐	16		☒								
2/7		☐	☐	17		☒								
2/8		☐	☐	18		☒								

Activate
Save As...
Refresh
Canc

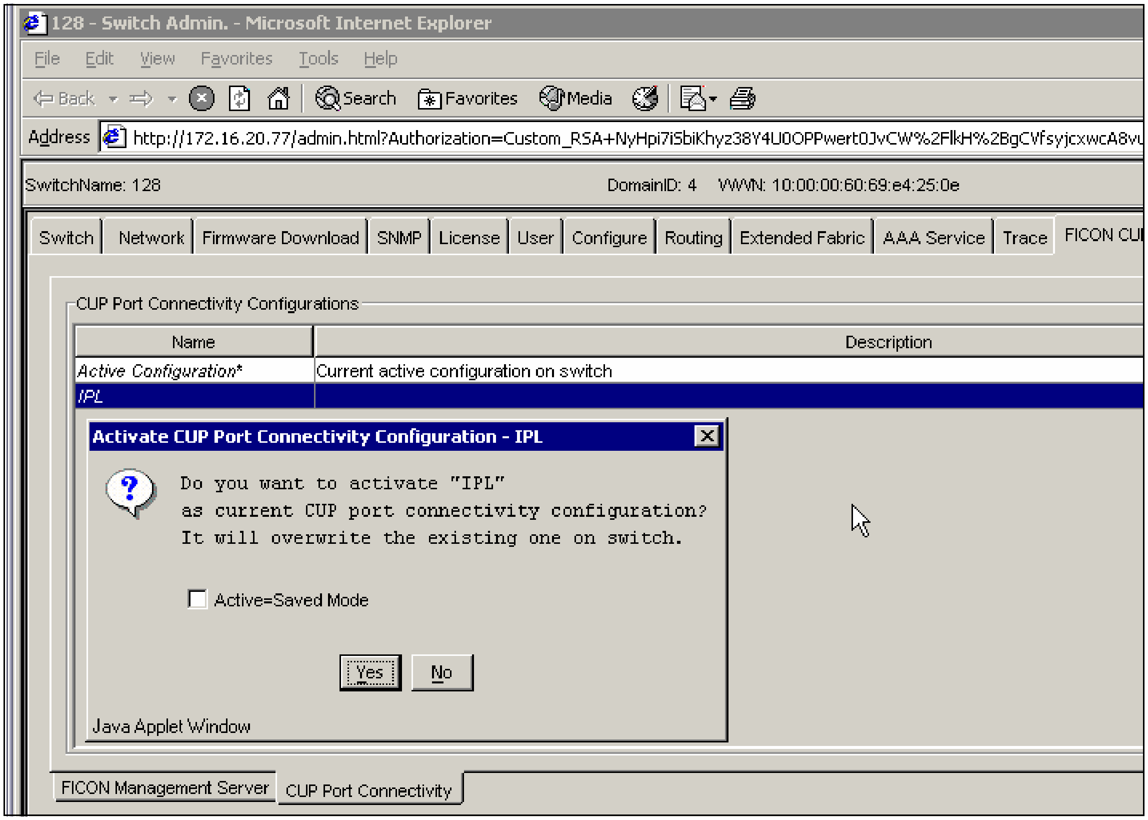
Figure 1-292 Port connectivity matrix

Activating CUP port connectivity

When you activate a saved CUP port connectivity configuration on the switch, the preceding configuration (the one that is currently active) is overwritten.

To activate a saved CUP port connectivity configuration, display the CUP port connectivity configuration list, click to select the saved configuration from the list, and click **Activate**.

The Activate CUP Port Connectivity Configuration confirmation dialog displays as shown in Figure 1-293. The dialog reminds you that the current configuration will be overwritten upon activation.


128 - Switch Admin. - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Address
Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUI
CUP Port Connectivity Configurations
Activate CUP Port Connectivity Configuration - IPL
Yes
No
Java Applet Window
FICON Management Server
CUP Port Connectivity

http://172.16.20.77/admin.html?Authorization=Custom_RSA+NyHpi7iSbiKhyz38Y4U0OPPwert0JvCW%2FlkH%2BgCVfsyjcxwcA8vu

SwitchName: 128 DomainID: 4 WWN: 10:00:00:60:69:e4:25:0e

Name	Description
*Active Configuration**	Current active configuration on switch
IPL	

Do you want to activate "IPL"
as current CUP port connectivity configuration?
It will overwrite the existing one on switch.

☐ Active=Saved Mode

Figure 1-293 Confirm dialog

Optionally, click **Active=Saved Mode** to enable (if checked) or disable (if unchecked) the Active=Saved FMS parameter after the configuration is activated.

Click **Yes** to activate the configuration, or click **No** to cancel the activation.

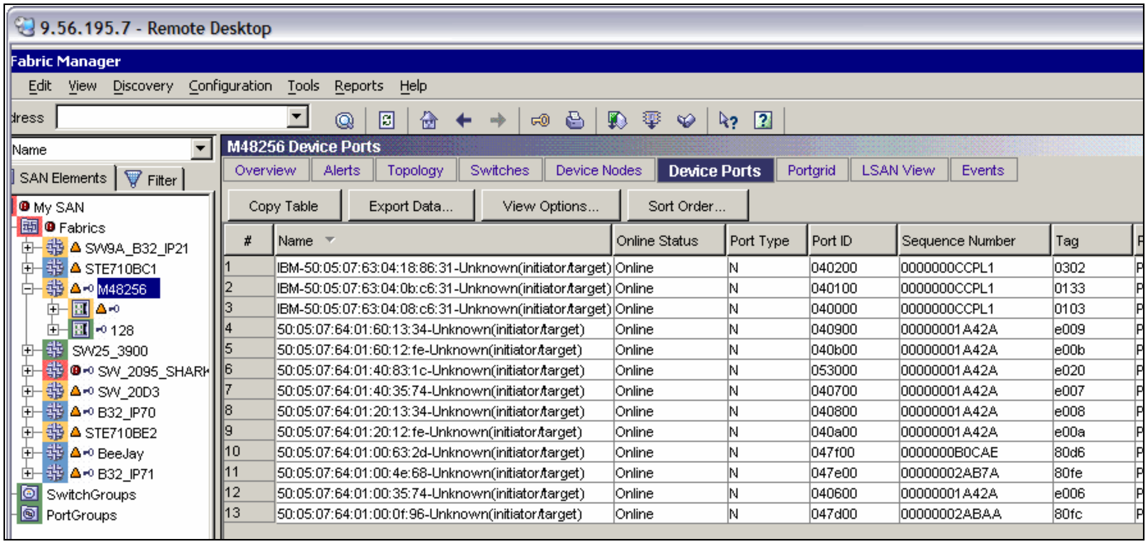
1.14.6 Zoning and PDCM considerations

The FICON Prohibit Dynamic Connectivity Mask (PDCM) controls whether or not communication between a pair of ports in the switch is prohibited or allowed. If there are any differences in restrictions set up with zoning and PDCM, the most restrictive rules are automatically applied.

All FICON devices should be configured in a single zone using the “Domain, Area” notation. PDCM can then be used to “Allow” or “Prohibit” access between specific port pairs. PDCM persists across a failover because it is replicated at all times to the standby CP blade. The active PDCM configuration is saved to the IPL if Active=Saved Mode has been enabled.

1.14.7 Displaying and configuring ports

We show some of the functions that can be performed at a port level. First we select our fabric and then click the **Device Ports** tab as shown in Figure 1-294, to list all the ports in our fabric.

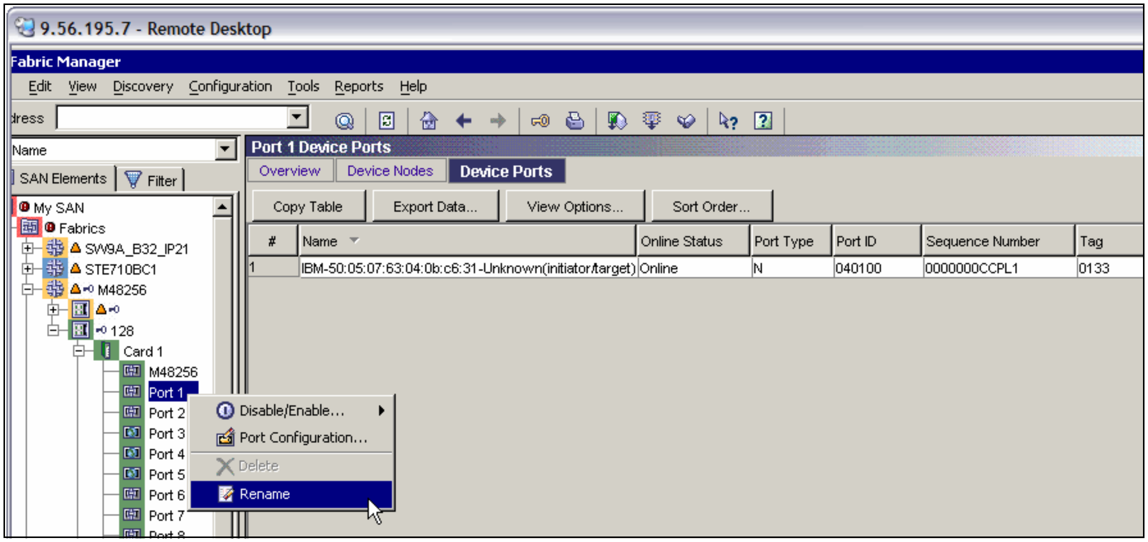

9.56.195.7 - Remote Desktop
Fabric Manager
Edit
View
Discovery
Configuration
Tools
Reports
Help
dress
Name
SAN Elements
Filter
My SAN
Fabrics
SW9A_B32_IP21
STE710BC1
M48256
128
SW25_3900
SW_2095_SHARK
SW_20D3
B32_IP70
STE710BE2
BeeJay
B32_IP71
SwitchGroups
PortGroups
M48256 Device Ports
Overview
Alerts
Topology
Switches
Device Nodes
Device Ports
Portgrid
LSAN View
Events
Copy Table
Export Data...
View Options...
Sort Order...

#	Name	Online Status	Port Type	Port ID	Sequence Number	Tag
1	IBM-50:05:07:63:04:18:86:31-Unknown(initiator/target)	Online	N	040200	0000000CCPL1	0302
2	IBM-50:05:07:63:04:0b:c6:31-Unknown(initiator/target)	Online	N	040100	0000000CCPL1	0133
3	IBM-50:05:07:63:04:08:c6:31-Unknown(initiator/target)	Online	N	040000	0000000CCPL1	0103
4	50:05:07:64:01:60:13:34-Unknown(initiator/target)	Online	N	040900	00000001A42A	e009
5	50:05:07:64:01:60:12:fe-Unknown(initiator/target)	Online	N	040b00	00000001A42A	e00b
6	50:05:07:64:01:40:83:1c-Unknown(initiator/target)	Online	N	053000	00000001A42A	e020
7	50:05:07:64:01:40:35:74-Unknown(initiator/target)	Online	N	040700	00000001A42A	e007
8	50:05:07:64:01:20:13:34-Unknown(initiator/target)	Online	N	040800	00000001A42A	e008
9	50:05:07:64:01:20:12:fe-Unknown(initiator/target)	Online	N	040a00	00000001A42A	e00a
10	50:05:07:64:01:00:63:2d-Unknown(initiator/target)	Online	N	047f00	0000000B0CAE	80d6
11	50:05:07:64:01:00:4e:68-Unknown(initiator/target)	Online	N	047e00	00000002AB7A	80fe
12	50:05:07:64:01:00:35:74-Unknown(initiator/target)	Online	N	040600	00000001A42A	e006
13	50:05:07:64:01:00:0f:96-Unknown(initiator/target)	Online	N	047d00	00000002ABAA	80fc

Figure 1-294 Device Ports display for fabric

As can be seen, the ports are identified by a WWN (its 8-byte hexadecimal representation) as its predefined port name. The predefined port name has no information with respect to the port itself, or the connected devices. It makes sense to give it a meaningful name to identify the port, or the device that is connected to the port, or both. To assign a name to a port, we select a port from the left hand view, right-click, and we get the pop-up shown in Figure 1-295.

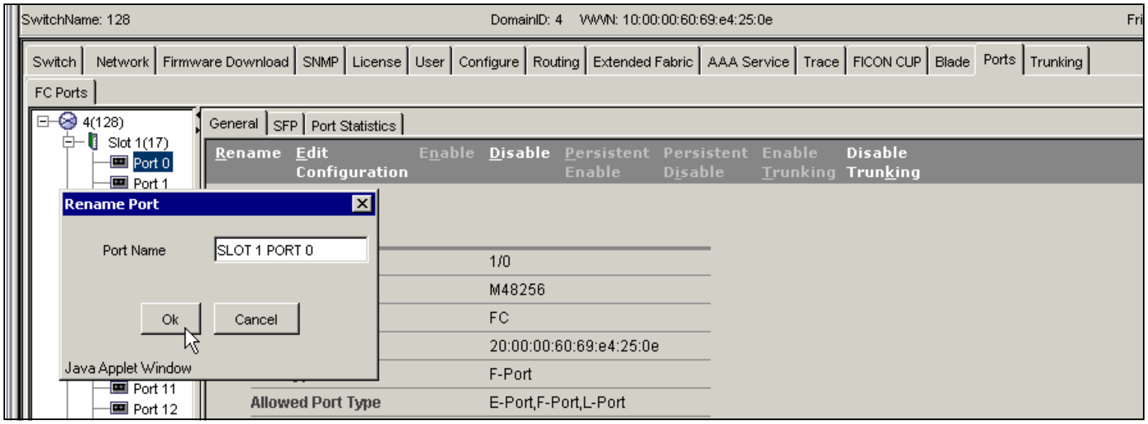
> **Note:** A Port Type of “N” indicates that the connected device is either a FICON channel, or a FICON capable control unit.


9.56.195.7 - Remote Desktop
Fabric Manager
Edit View Discovery Configuration Tools Reports Help
dress
Name
SAN Elements
Filter
My SAN
Fabrics
SW9A_B32_IP21
STE710BC1
M48256
128
Card 1
M48256
Port 1
Port 2
Port 3
Port 4
Port 5
Port 6
Port 7
Port 8
Disable/Enable...
Port Configuration...
Delete
Rename
Port 1 Device Ports
Overview
Device Nodes
Device Ports
Copy Table
Export Data...
View Options...
Sort Order...

#	Name	Online Status	Port Type	Port ID	Sequence Number	Tag
1	IBM-50:05:07:63:04:0b:c6:31-Unknown(initiator/target)	Online	N	040100	0000000CCPL1	0133

Figure 1-295 Rename port (1st method)

We simply type in the name of the port that we require. An alternative method is to rename the port by clicking the **Ports** tab, and then selecting the port we want to rename, and then clicking **Rename** under the General tab. This is shown in Figure 1-296.


Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Blade
Ports
Trunking
Fri
FC Ports
4(128)
Slot 1(17)
Port 0
Port 1
Port 11
Port 12
General
SFP
Port Statistics
Rename
Edit Configuration
Enable
Disable
Persistent Enable
Persistent Disable
Enable Trunking
Disable Trunking
Rename Port
Ok
Cancel
Java Applet Window

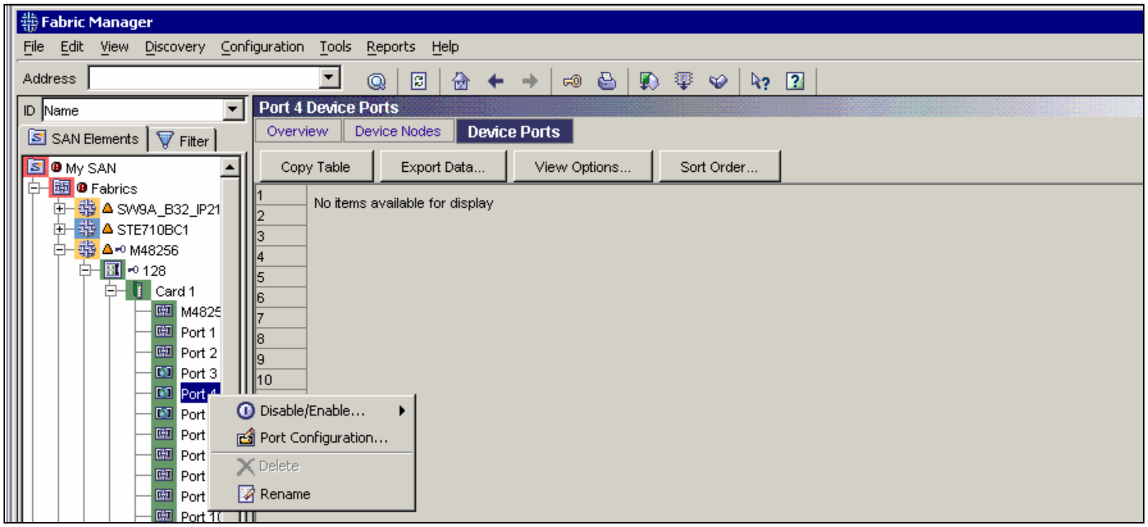
SwitchName: 128 DomainID: 4 WWN: 10:00:00:60:69:e4:25:0e

Port Name: SLOT 1 PORT 0

1/0
M48256
FC
20:00:00:60:69:e4:25:0e
F-Port
Allowed Port Type E-Port,F-Port,L-Port

Figure 1-296 Rename port (2nd method)

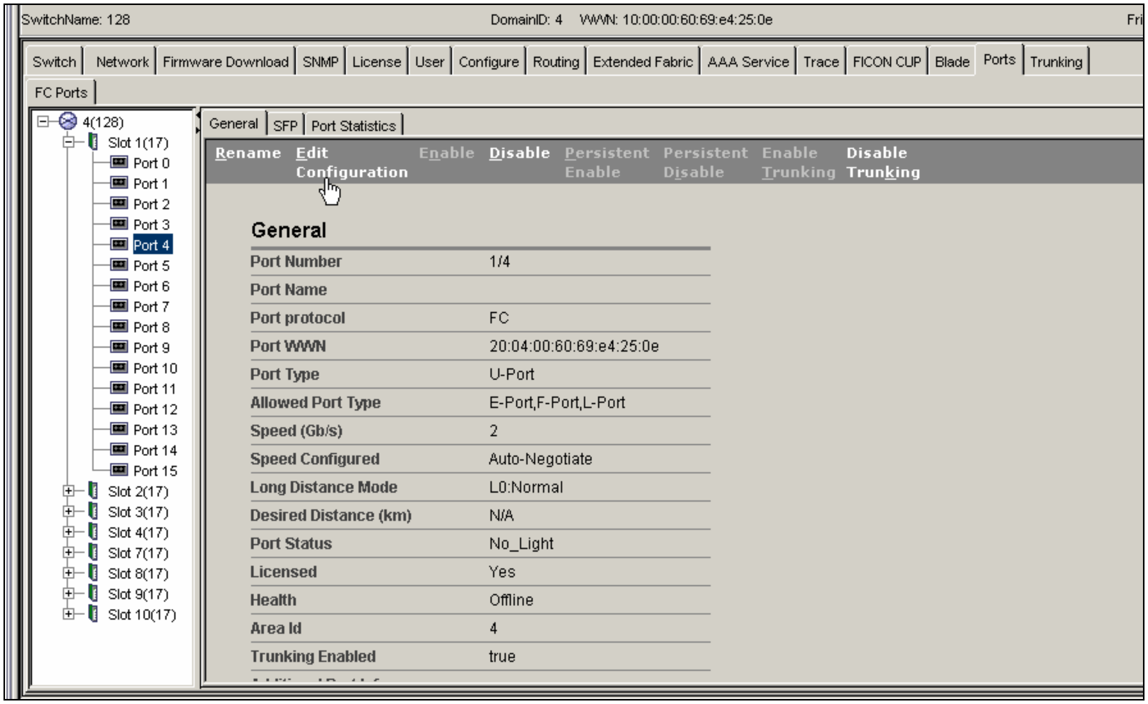
If we return to the Device Ports view, we can also start the Port Configuration wizard as shown in Figure 1-297.


Fabric Manager
File Edit View Discovery Configuration Tools Reports Help
Address
ID Name
SAN Elements
Filter
My SAN
Fabrics
SW9A_B32_IP21
STE710BC1
M48256
128
Card 1
M4825
Port 1
Port 2
Port 3
Port 4
Port
Port
Port
Port
Port
Port 1(
Port 4 Device Ports
Overview
Device Nodes
Device Ports
Copy Table
Export Data...
View Options...
Sort Order...
1
2
3
4
5
6
7
8
9
10
Disable/Enable...
Port Configuration...
Delete
Rename

No items available for display

Figure 1-297 Port configuration

A new pop-up menu appears as shown in Figure 1-298.


Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Blade
Ports
Trunking
FC Ports
4(128)
Slot 1(17)
Port 0
Port 1
Port 2
Port 3
Port 4
Port 5
Port 6
Port 7
Port 8
Port 9
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15
Slot 2(17)
Slot 3(17)
Slot 4(17)
Slot 7(17)
Slot 8(17)
Slot 9(17)
Slot 10(17)
General
SFP
Port Statistics
Rename
Edit Configuration
Enable
Disable
Persistent Enable
Persistent Disable
Enable Trunking
Disable Trunking
Fri

SwitchName: 128 DomainID: 4 WWN: 10:00:00:60:69:e4:25:0e

General

Port Number	1/4
Port Name	
Port protocol	FC
Port WWN	20:04:00:60:69:e4:25:0e
Port Type	U-Port
Allowed Port Type	E-Port,F-Port,L-Port
Speed (Gb/s)	2
Speed Configured	Auto-Negotiate
Long Distance Mode	L0:Normal
Desired Distance (km)	N/A
Port Status	No_Light
Licensed	Yes
Health	Offline
Area Id	4
Trunking Enabled	true

Figure 1-298 Edit configuration

There are three tabs available along with a number of options. The available options will appear in white and are clickable. Those that are not available appear grayed out. We click **Edit Configuration** to start the FC Port Configuration wizard as shown in Figure 1-299.

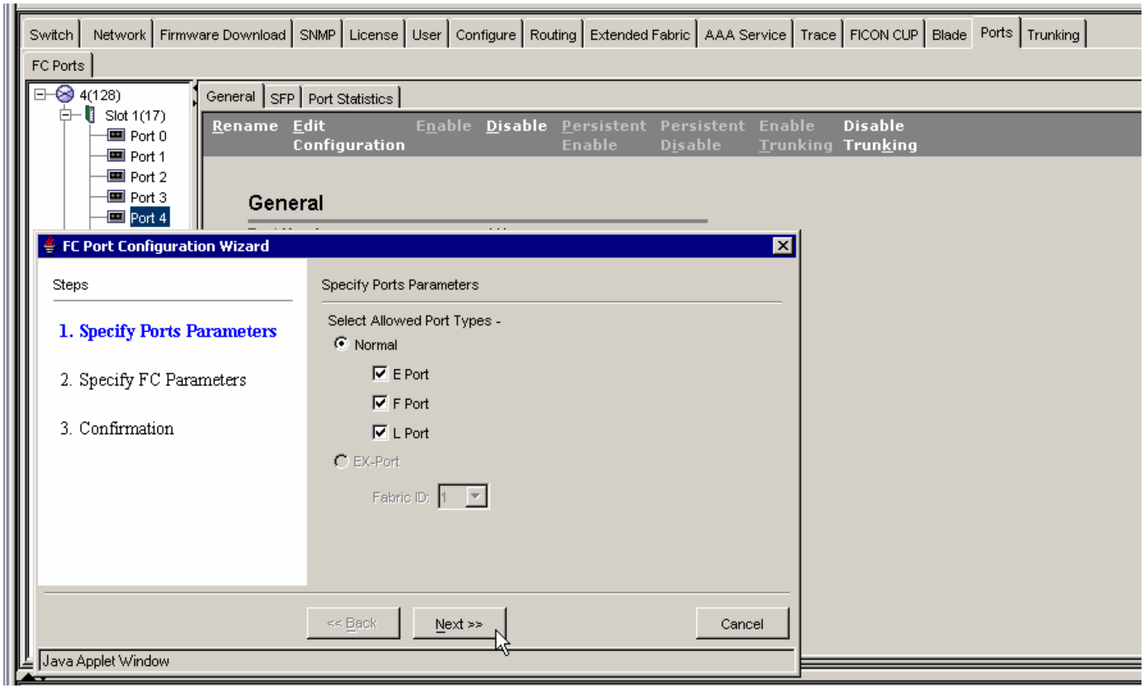
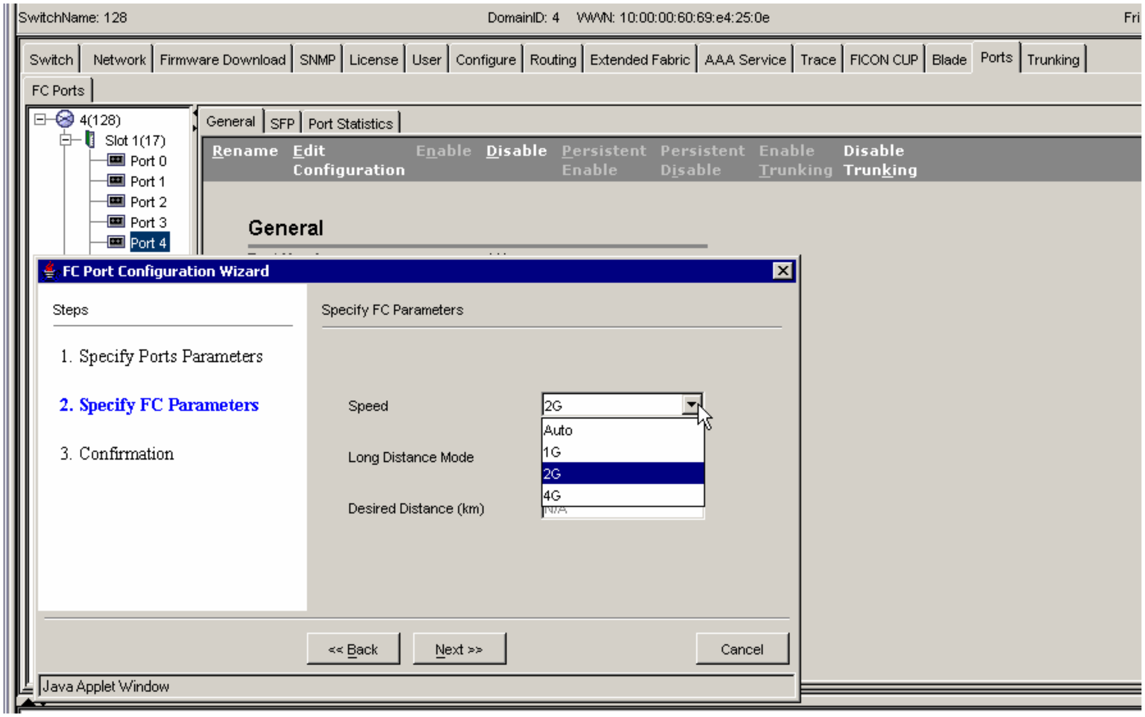

Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Blade
Ports
Trunking
FC Ports
4(128)
Slot 1(17)
Port 0
Port 1
Port 2
Port 3
Port 4
General
SFP
Port Statistics
Rename
Edit Configuration
Enable
Disable
Persistent Enable
Persistent Disable
Enable Trunking
Disable Trunking
General
FC Port Configuration Wizard
Steps
1. Specify Ports Parameters
2. Specify FC Parameters
3. Confirmation
Specify Ports Parameters
Select Allowed Port Types -
● Normal
☑ E Port
☑ F Port
☑ L Port
○ EX-Port
Fabric ID: 1
<< Back
Next >>
Cancel
Java Applet Window

Figure 1-299 Port configuration wizard

We can select the port attributes; when done, we click **Next** and get the pop-up menu shown in Figure 1-300.


SwitchName: 128
DomainID: 4
WWN: 10:00:00:60:69:e4:25:0e
Fri
Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Blade
Ports
Trunking
FC Ports
4(128)
Slot 1(17)
Port 0
Port 1
Port 2
Port 3
Port 4
General
SFP
Port Statistics
Rename
Edit Configuration
Enable
Disable
Persistent Enable
Persistent Disable
Enable Trunking
Disable Trunking
General
FC Port Configuration Wizard
Steps
1. Specify Ports Parameters
2. Specify FC Parameters
3. Confirmation
Specify FC Parameters
Auto
1G
2G
4G
<< Back
Next >>
Cancel
Java Applet Window

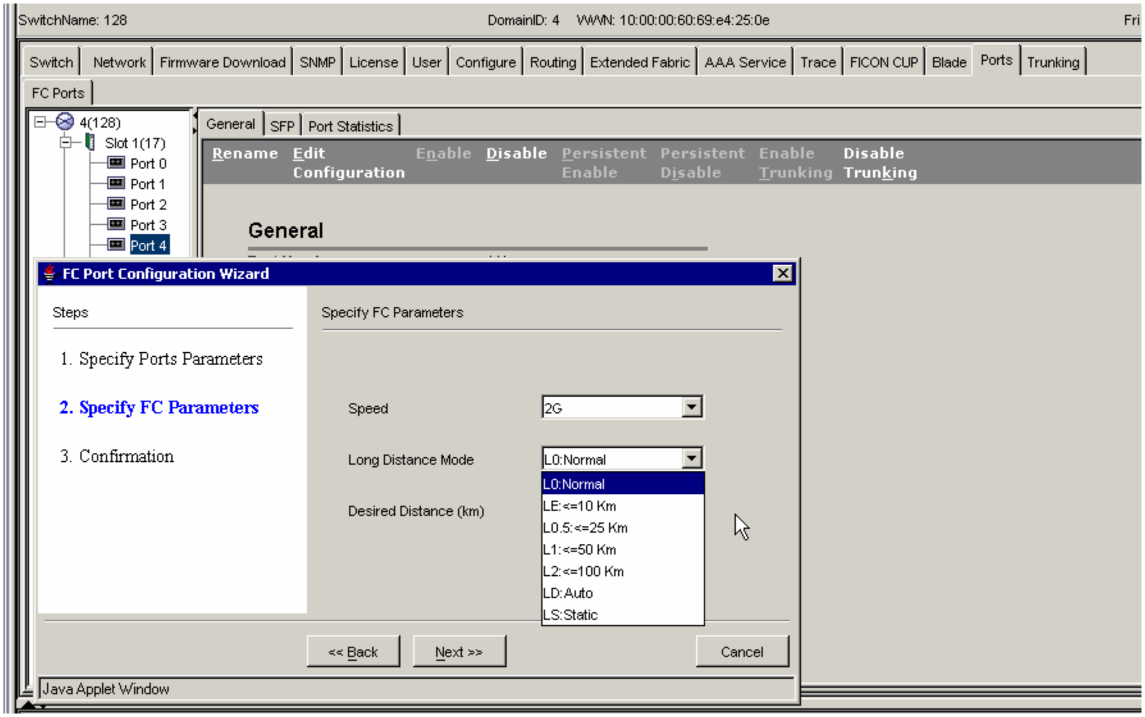
Speed: 2G

Long Distance Mode

Desired Distance (km): N/A

Figure 1-300 Specify parameters

Here we can specify the Speed and Long Distance parameters that we require, as shown in Figure 1-301.


SwitchName: 128
DomainID: 4
WWN: 10:00:00:60:69:e4:25:0e
Fri
Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Blade
Ports
Trunking
FC Ports
4(128)
Slot 1(17)
Port 0
Port 1
Port 2
Port 3
Port 4
General
SFP
Port Statistics
Rename
Edit Configuration
Enable
Disable
Persistent Enable
Persistent Disable
Enable Trunking
Disable Trunking
General
FC Port Configuration Wizard
Steps
1. Specify Ports Parameters
2. Specify FC Parameters
3. Confirmation
<< Back
Next >>
Cancel
Java Applet Window

Specify FC Parameters

Speed: 2G

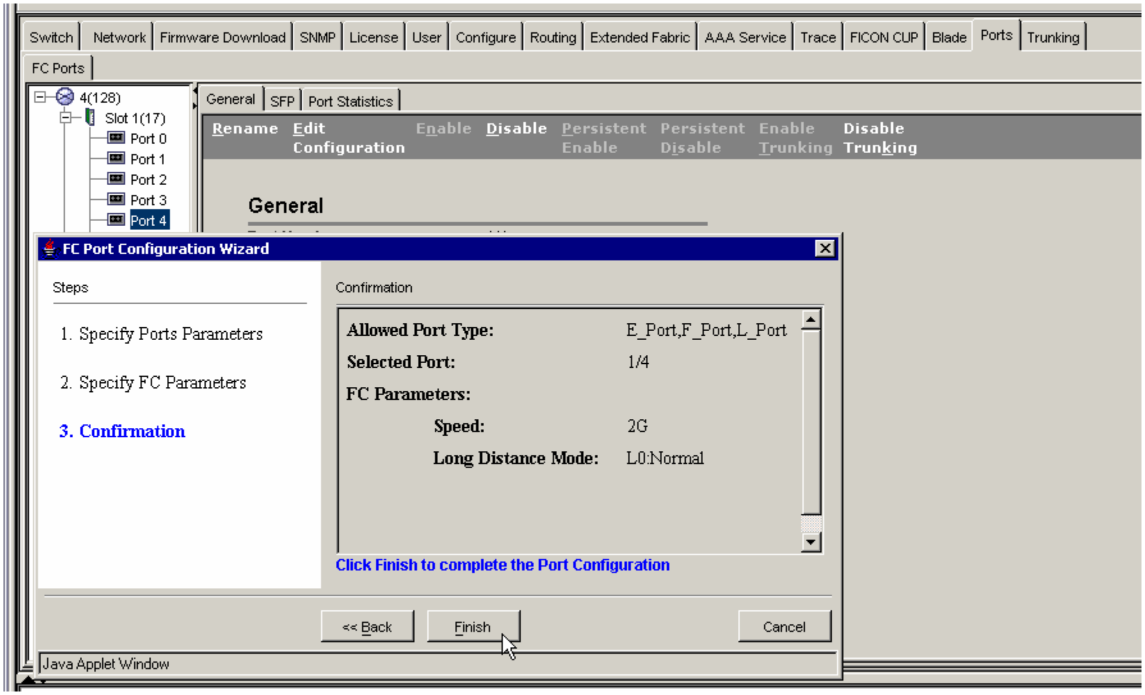
Long Distance Mode: L0:Normal

- L0:Normal
- LE:<=10 Km
- L0.5:<=25 Km
- L1:<=50 Km
- L2:<=100 Km
- LD:Auto
- LS:Static

Desired Distance (km)

Figure 1-301 Distance settings

When we have selected the settings we want, we click **Finish** to complete the wizard as shown in Figure 1-302.


Switch
Network
Firmware Download
SNMP
License
User
Configure
Routing
Extended Fabric
AAA Service
Trace
FICON CUP
Blade
Ports
Trunking
FC Ports
4(128)
Slot 1(17)
Port 0
Port 1
Port 2
Port 3
Port 4
General
SFP
Port Statistics
Rename
Edit Configuration
Enable
Disable
Persistent Enable
Persistent Disable
Enable Trunking
Disable Trunking
General
FC Port Configuration Wizard
Steps
1. Specify Ports Parameters
2. Specify FC Parameters
3. Confirmation
Confirmation
<< Back
Finish
Cancel
Java Applet Window

Allowed Port Type: E_Port,F_Port,L_Port

Selected Port: 1/4

FC Parameters:

Speed: 2G

Long Distance Mode: L0:Normal

Click Finish to complete the Port Configuration

Figure 1-302 Confirmation

We are also able to Disable/Enable the port as can be seen in Figure 1-303.

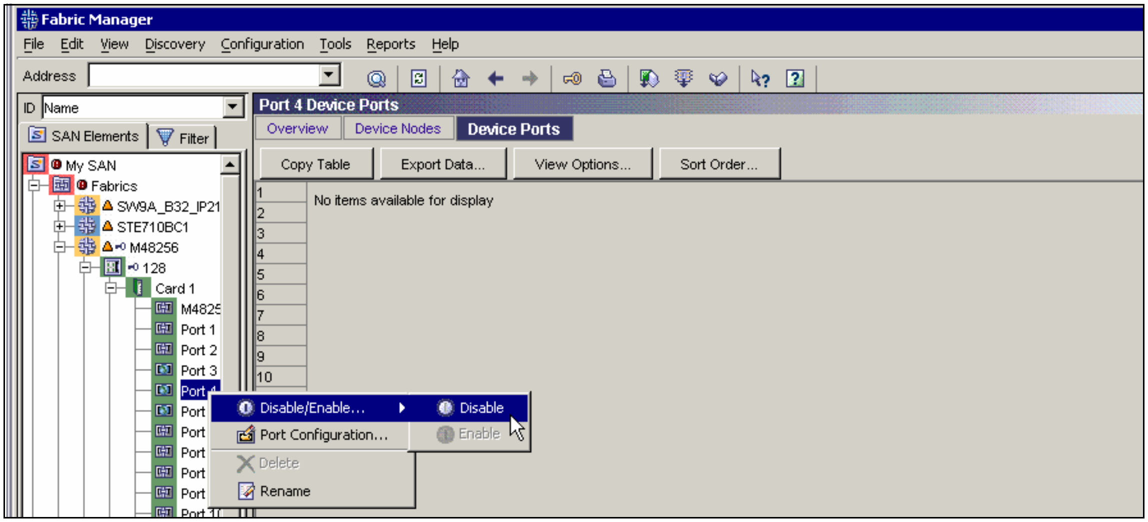
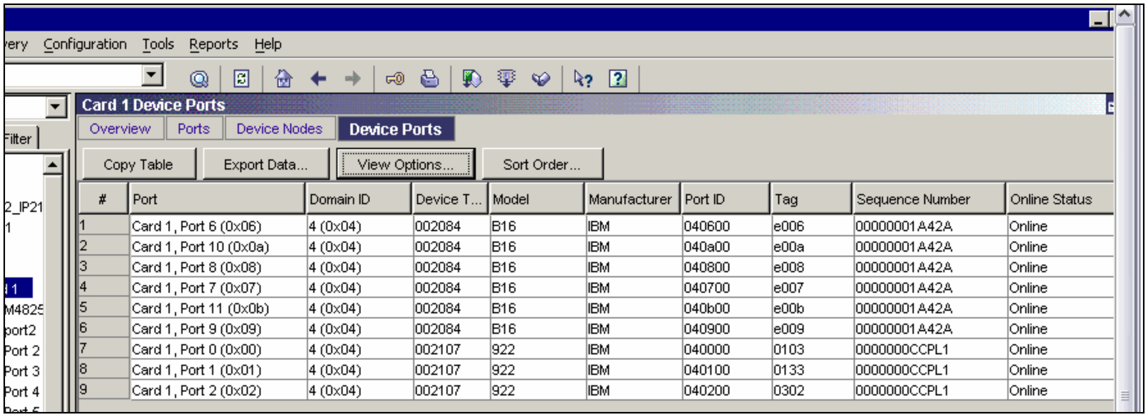

Fabric Manager
File Edit View Discovery Configuration Tools Reports Help
Address
ID Name
SAN Elements
Filter
My SAN
Fabrics
SW9A_B32_IP21
STE710BC1
M48256
128
Card 1
M4825
Port 1
Port 2
Port 3
Port 4
Port 4 Device Ports
Overview
Device Nodes
Device Ports
Copy Table
Export Data...
View Options...
Sort Order...
No items available for display
Disable/Enable...
Port Configuration...
Delete
Rename
Disable
Enable

Figure 1-303 Disable/Enable port

FICON view

You are able to sort the view (by clicking **View Options**) to suit your own particular requirements. One display that we have found useful is shown in Figure 1-304.


Configuration Tools Reports Help
Card 1 Device Ports
Overview
Ports
Device Nodes
Device Ports
Copy Table
Export Data...
View Options...
Sort Order...

#	Port	Domain ID	Device T...	Model	Manufacturer	Port ID	Tag	Sequence Number	Online Status
1	Card 1, Port 6 (0x06)	4 (0x04)	002084	B16	IBM	040600	e006	00000001A42A	Online
2	Card 1, Port 10 (0x0a)	4 (0x04)	002084	B16	IBM	040a00	e00a	00000001A42A	Online
3	Card 1, Port 8 (0x08)	4 (0x04)	002084	B16	IBM	040800	e008	00000001A42A	Online
4	Card 1, Port 7 (0x07)	4 (0x04)	002084	B16	IBM	040700	e007	00000001A42A	Online
5	Card 1, Port 11 (0x0b)	4 (0x04)	002084	B16	IBM	040b00	e00b	00000001A42A	Online
6	Card 1, Port 9 (0x09)	4 (0x04)	002084	B16	IBM	040900	e009	00000001A42A	Online
7	Card 1, Port 0 (0x00)	4 (0x04)	002107	922	IBM	040000	0103	0000000CCPL1	Online
8	Card 1, Port 1 (0x01)	4 (0x04)	002107	922	IBM	040100	0133	0000000CCPL1	Online
9	Card 1, Port 2 (0x02)	4 (0x04)	002107	922	IBM	040200	0302	0000000CCPL1	Online

Figure 1-304 FICON display

In Figure 1-304 on page 376:

Port identifies its physical location in the switch by its card and slot position. The associated hexadecimal value is the port address used to address the port.

Domain ID shows the switch domain ID in both decimal, 4, and hexadecimal, (0x04). Be aware that the hexadecimal value is used to define the switch in HCD.

Device Type shows the connected device type.

Model identifies the model number.

Manufacturer identifies the manufacturer of the connected device.

Port ID is the hexadecimal representation of the 2-byte link address used by the FICON protocol to address the switch and the port.

Tag is a hexadecimal 2-byte value; the first byte is the CHPID, and the second byte is the port.

Sequence Number is the serial number of the attached device.

Online Status is the online status of the connected device.

These are the basic steps to get started with FICON.

2

Implementing a SAN with the m-type family

In this chapter we cover the implementation of the IBM TotalStorage m-type family of Fibre Channel switches and directors, which are provided under an OEM agreement with McDATA Corporation. We review the features and characteristics of the product set, including the management options, and then show how to install and configure the products.

We also show how to use some of the many security features available, how to configure the various optional features, and how to perform zoning. Finally, we cover issues relating to multiple switch environments and basic troubleshooting.

© Copyright IBM Corp. 1999-2007. All rights reserved.

2.1 Product introduction

The IBM TotalStorage SAN m-type family of products extends from entry-level switches to large enterprise class directors, including SAN router models, and is capable of providing solutions for all SAN requirements. The products are all fully interoperable, and provide investment protection when a SAN grows.

In this chapter we provide an overview of the m-type family, plus details of all the available features and functions. We also cover management, security, implementation issues, and finally, basic troubleshooting.

Further details of current products can be obtained at the following Web site:

`http://www-1.ibm.com/servers/storage/san/m_type/`

2.1.1 Hardware

In Table 2-1 we list the m-type family products, along with their equivalent McDATA names.

Table 2-1 IBM TotalStorage SAN m-type product family

IBM name	IBM type and model	McDATA name
IBM TotalStorage SAN16M-2 Express model	2026-16E	Sphereon 4400
IBM TotalStorage SAN16M-2 fabric switch	2026-416	Sphereon 4400
IBM TotalStorage SAN32M-2 Express model	2026-32E	Sphereon 4700
IBM TotalStorage SAN32M-2 fabric switch	2026-432	Sphereon 4700
IBM TotalStorage SAN04M-R	2027-R04	Eclipse 1620
IBM TotalStorage SAN16M-R	2027-R16	Eclipse 2640
IBM TotalStorage SAN140M	2027-140	Intrepid 6140
IBM TotalStorage SAN256M	2027-256	Intrepid i10K

More in-depth descriptions of these products can be found in the Redbooks publication, *IBM TotalStorage: SAN Product, Design, and Optimization Guide*, SG24-6384.

IBM TotalStorage SAN16M-2 Fabric Switch

Figure 2-1 shows the SAN16M-2 Fabric Switch.

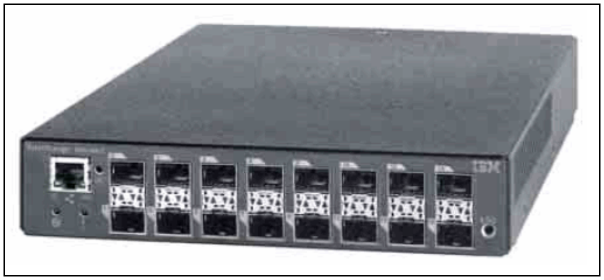


Figure 2-1 SAN16M-2

The IBM TotalStorage SAN16M-2 is controlled by single control processor (CTP) card. It provides ports for shortwave transceivers, offers minimal eight up to sixteen non-blocking ports providing 1, 2 and 4 Gbps Fibre Channel Arbitrated Loop (FC-AL) and Fabric (FC-SW) operation. The switch uses auto-sensing and auto-negotiating ports, allows clients to purchase connectivity in four-port increments, and provides integrated support for full fabric and FC-AL tape attachment to core fabric switches and directors. The switch is half-rack width configuration and can be non-rack installed (desktop). The SAN16M-2 is delivered with one external power supply.

The switch versions include entry level 8-port and 12-port switches, and a midrange 16-port edge switch. The entry switch versions consists of eight shortwave ports. Each port is self-configuring as a fabric, fabric loop or expansion port. The switch provides scalable upgrades, in 4-port increments, without fabric disruption.

The 2026-16E is an entry level switch, therefore it is not designed to be as highly available as, for example, the 2026-224. It consists of a single CTP card. If any component on the CTP card fails, the entire switch must be replaced. Optionally, a second external power supply can be installed. By installing the second power supply, the 2026-16E automatically enables high availability (HA) mode, which allows any of the two power supplies to be replaced without switch downtime. Each power supply provides a separate connection to the CTP card to allow for independent power sources. The 2026-16E is equipped with three internal fans to provide cooling for the CTP card. The switch remains operational if one of the three fans fails.

IBM TotalStorage SAN32M-2 Fabric Switch

Figure 2-2 shows the SAN32M-2 Fabric Switch.

Figure 2-2 SAN32M-2

The IBM TotalStorage SAN32M-2 provides ports for longwave and shortwave transceivers. Shortwave SFPs offer a minimum of sixteen scaling up to thirty-two non-blocking ports providing 1, 2 and 4 Gbps Fibre Channel Arbitrated Loop (FC-AL) and Fabric (FC-SW) operation. Longwave SFPs operate at 2 Gbps speed. The switch uses auto-sensing and auto-negotiating ports, allows clients to purchase connectivity in eight-port increments, and provides integrated support for full fabric and FC-AL tape attachment to core fabric switches and directors. The switch is 1U rack width and can be non-rack installed (desktop), or installed into an SANC40M cabinet, or an industry standard 19" rack. The switch has dual power supplies.

The switch versions include a midrange 16-port and enterprise 24 and 32-port edge switch. The midrange switch version consists of sixteen shortwave ports. Each port is self-configuring as a fabric, fabric loop, or expansion port. Optional long wave SFPs at 2 Gbps speed can be ordered separately. The switch provides scalable upgrades, in 8-port increments, without fabric disruption. Each FlexPort upgrade consists of eight shortwave SFP transceivers and an activation key which adds eight ports to the fabric switch.

The SAN32M-2 is a midrange to enterprise level switch. It consists of single CTP card. If any component on the CTP card fails, the entire switch must be replaced. It is delivered with two hot-swappable, redundant power supplies that allow the switch to remain online if one supply fails. Dual power cords enable attachment to independent power sources to improve availability.

A hot-swappable power supply eliminates downtime for service when replacing a failed component and eliminates the risk of erroneously cabling a replacement switch because of a simple component failure. Each power supply has three cooling fans. The switch remains operational if one of these three fans fails. Fans themselves are not field replaceable units (FRUs), and the entire power supply has to be replaced.

IBM TotalStorage SAN140M Director

Figure 2-3 shows the SAN140M Director.

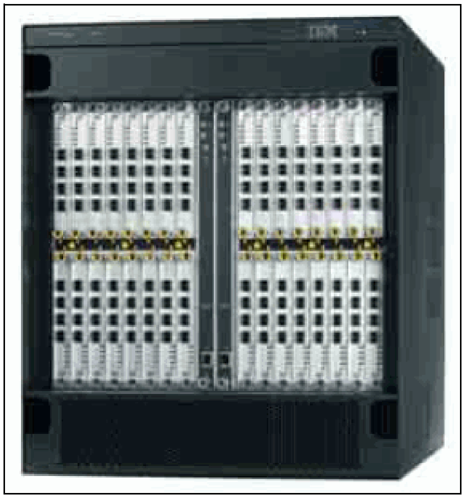


Figure 2-3 SAN140M

The IBM TotalStorage SAN140M, is a 140-port product that provides dynamic switched connections between Fibre Channel servers and devices in a SAN environment.It is 12U high, so up to three can be configured in an SANC40M cabinet equipment cabinet, providing up to 420 ports in a single cabinet. The IBM TotalStorage SAN140M, shown in Figure 2-3, provides 140-port, high availability switching and enterprise-level scalability for data center class core/edge fabrics, and long transmission distances (up to 35 km, or up to 100 km with repeaters).

Each director comes with a minimum of four 4-port UPM (Universal Port Modules) consisting of 16 G_Ports. The IBM TotalStorage SAN140M is capable of supporting from 16 up to 140 ports by adding additional UPMs. The ability to support different port types aids in building a scalable environment.

There is an extended distance option that can be configured on a port by port basis. The extended distance option is used to assign 60 additional buffers to the specified port in order to support operation at distances of up to 100 km using repeaters. Additionally, an XPM blade can be inserted to any available UPM slot. Each XPM module provides one shortwave or longwave 10 Gbps port using the XFP transceivers. Shortwave XFP transceiver supports distances up to 82 meters over standard 50 micron multimode fiber. Longwave XFP supports up to 10 km over 9 micron single mode fibre or up to 100 km with repeaters.

Pairs of critical field replaceable units (FRUs) installed in the director provide redundancy in the event that an FRU fails. When an active FRU fails, the backup FRU takes over operation automatically by failover processing to maintain director and Fibre Channel link operation.

IBM TotalStorage SAN256M Director

Figure 2-4 shows the SAN256M Director.

Figure 2-4 SAN256M

The IBM TotalStorage SAN256M, also known as the i10K, is designed to provide up to 8 Line Modules (LIM), each with up to 32 Fibre Channel (FC) ports. A fully-populated SAN256M is comprised of up to 256 FC ports in a 14U rack mount chassis. A variety of LIM types are available that enable a combination of 2/4-Gbps FC ports for connection to server and storage resources, as well as 10-Gbps FC ports for Inter- Switch Link (ISL) between SAN256M directors. This flexibility enables growth from 64 to 256 FC ports, or the addition of 10-Gbps FC ISL connectivity. Optionally, clients can purchase two additional switching modules (SWMs) and the Fiber Connection (FICON) management server.

The chassis supports from two to eight line modules (LIMs), each holding four paddles. Each paddle provides either eight 2-Gbps ports or two 10-Gbps ports, in either shortwave or longwave. Using one 10-Gbps port as an ISL can replace six 4Gbps ISL ports. The director is managed by EFCM in the same way as other McDATA switches and directors, with the same look and feel.

The SAN256M can be dynamically partitioned from one to four separate directors, each with its own management and Fibre Channel services subsystems. The director scales from 32 to 256 1 Gbps, 2 and 4 Gbps Fibre Channel ports. When configured for 10 Gbps, up to 32 ports can be configured.

The director has a scalable switching infrastructure. The combination of high port count and partitioning enables enterprise data centers to use the director for small and large SAN fabrics. Fabrics built with the director require fewer inter-switch links (ISLs). Large fabrics benefit from deterministic non-blocking performance not possible with smaller switches interconnected with ISLs.

Smaller fabrics benefit from better resource utilization because they do not have to be over-provisioned for future growth. Dynamic partitioning enables additional fabric ports to be added to a partition without interrupting traffic on the fabric. The director comes with director-class reliability and performance features including redundant switching modules, redundant control processor (CTP) cards for traffic management, redundant power supplies, hot code load, and activation for all CTP software. Most of the director components are hot-swappable.

The director supports the McDATA non-blocking extendable open network (EON) architecture and concurrent firmware downloads through hot code activation (HotCAT) technology. Up to two directors can be configured to order in a SANC40M cabinet, thus providing up to 512 ports in a single cabinet. The director can be managed through a rack-mount management server running a Java-based SAN management application EFCM 9.0 and the GUI-based Intrepid 10000 Element Manager application.

The director provides a modular design that enables quick removal and replacement of FRUs. The director FRUs can be accessed from the front, and include the following components:

- Control processor (CTP) cards
- Line modules (LIMs)
- 1 or 2-Gbps optical paddles (OTPS)
- 10-Gbps optical paddles (OTPX)
- 1,2 or 4-Gbps small form-factor pluggable (SFP) transceivers
- 10-Gbps form-factor pluggable (XFP) transceivers
- Front fan trays (FTF/FBF)
- Cabletrays
- Optical paddle and LIM filler panels

Director FRUs accessed from the rear include these components:

- Switching modules (SWMs)
- Rear fan trays (RTF/RBF)
- Power supplies (PS)
- AC power switch/breaker
- SWM filler panels

2.1.2 Operating system

All m-type Fibre Channel switches prior to the IBM TotalStorage SAN256M run common firmware, namely the Enterprise Operating System (E/OS or E/OSc), whereas the IBM TotalStorage SAN256M runs a different version of firmware known as E/OSn. All devices support hot code load and activation (HotCAT), which enables firmware upgrades without impacting I/O operations.

The SAN04M-R and SAN16M-R run SAN router firmware, called Enterprise Operating System Internet working (E/OSi).

The process of upgrading firmware levels is shown later in this chapter.

2.1.3 Management tools

Following are the main management software GUIs available for the m-type family. The first two are part of the Enterprise Fabric Connectivity Manager (EFCM) software family, the other two are used for the configuration and management of the m-type SAN Router products.

- **EFCM Basic:** This was formerly known as SANpilot, and is a free Web browser based management tool that is a standard part of the firmware. It is suitable for small fabrics which do not contain directors, although it is provided with all products.
- **EFCM:** This is a Java based server product which provides a fabric-wide management solution. A dedicated server is required to host the software, which can manage multiple fabrics.

  Individual m-type switches are managed from the EFCM by launching the Element Manager GUI for the relevant switch or director.

  Provided the principal switch in a fabric is an m-type switch, EFCM is capable of discovering non-McDATA switches in the fabric.

  Note: The EFCM server is required if your fabric contains directors, and is recommended if you have more than three switches.

- **SAN Router Element Manager:** This is a Web-based Java applet which is used to configure, manage and troubleshoot an individual SAN Router.
- **SANvergence Manager:** This is a Java-based collection of software tools used for the management and configuration of multiple SAN Routers in a SAN environment. The Element manger can be launched from SANvergence. Prior to EFCM V9.0, this software is loaded on a dedicated server, and can co-exist on an EFCM server.

Later in this chapter, we cover the installation and usage of the EFCM server and its clients.

Note: SANvergence Manager is included in EFCM from V9.0, and so is not required as a separate product.

All products also support a command line interface (CLI) and SNMP management by third-party management applications, as well as management via the SMI-S open standard.

2.1.4 Licensing

Many features are included in the base cost of the switch hardware, but some major features are optional, and require the purchase of additional licenses. These can either be obtained as part of the original purchase, or added later.

The full list of licensable features, together with the procedure for activating them, are covered later in the chapter.

2.1.5 Security

Essential security functions such as zoning and account administration are standard features. There are also optional advanced security functions such as SANtegrity Binding and SANtegrity Authentication, which can be purchased at additional cost.

2.2 Hardware

All switches and directors utilize hot-swappable SFP (LC connector) optics, which can be either shortwave or longwave. The ports are also auto-sensing and auto-negotiating for any of the speeds shown in Table 2-2, with the exception of 10 Gbps ports, which only connect to other 10 Gbps ports.

Table 2-2 IBM TotalStorage SAN m-type feature summary

Feature	**16M-2**	**32M-2**	**04M-R**	**16M-R**	**140M**	**256M**
Firmware OS	E/OS	E/OS	E/OSi	E/OSi	E/OS	E/OSn
Redundant power	S (d)	S	S	S	S	S
FlexPort increment	4	8	x	x	x	x
FC-AL	S	S	S	S	x	S
EFCM Enterprise	O	O	S	S	O	S
SANvergence Manager	x	x	S(e)	S(e)	x	x
Open Trunking	O	O (c)	x	x	O (c)	O(c)
SANtegrity Binding	O (b)	O (b)	x	x	O	S
SANtegrity Authentication	O (b)	O (b)	x	x	O	x
Port speeds (Gbps)	1, 2 & 4	1, 2 & 4	1	1,2	1,2 & 4	1,2 & 4
10 Gbps ISL	x	x	x	x	O	O
Preferred Pathing	S	S	x	x	S	S
Full Volatility	O	O	x	x	O	O
FICON CUP	x	O (a)	x	x	O	O
N_Port ID Virtualization	x	O (a)	x	x	O	x

n/a = Not applicable
S = Standard feature
O = Optional feature
x = Not supported
(a) Not on Express model
(b) Part of SANtegrity Enhanced
(c) Open Trunking supported for FICON as well as FCP
(d) Optional on Express model
(e) included in EFCM Enterprise from V9.0

2.2.1 Features

Tip: The hardware is shown and explained in more detail in *IBM TotalStorage: SAN Product, Design, and Optimization Guide*, SG24-6384.

Redundant power

Redundant power is provided by having two hot-swappable power supplies in the switch or director, along with the ability for the device to run on one failing power supply. In normal operation, the power supplies share the operating load. On the switches with internal power supplies, these include the fans used for cooling, and on the director switches there are separate redundant fan modules.

FlexPorts

This feature allows switches to be purchased at a low cost without all Fibre ports enabled. The Flexport Technology feature consists of an expansion kit that allows the upgrading of the switch, on demand, in four or eight port increments. The upgrade consists of a set of SFP transceivers and an activation key which adds ports to the fabric switch. The SFP transceivers are simply plugged into the switch, and the key used to activate them.

FC-AL

The ability to connect a FC-AL port to the switch or director is a characteristic of the hardware, and cannot be changed by purchasing a feature key.

Port speeds and 10 Gbps ISLs

SFPs capable of 1, 2, or 4 Gbps are auto-negotiating and automatically set themselves to the maximum speed supported by the link. If desired, the speed can be set manually to one of the supported speeds.

XFPs are capable of10 Gbps and as the encoding method is different from that of SFPs, they are not compatible with 1/2/4 Gbps ports. Such ports are also more expensive, and so are intended for ISLs.

Transceivers

SFP and XFP shortwave transceivers provide connection for multimode cable with a core diameter of 50 or 62.50 microns. These are used primarily for short distance connections.

SFP and XFP longwave laser transceivers provide connection for single mode cable with a core diameter of 9 micron. These are used for long distance connection.

Shortwave ports can only connect to other shortwave ports, and the same applies to longwave ports.

In the m-type switches, all transceivers are hot pluggable.

Predictive optic monitoring

Newer SFPs and XFPs support monitoring of their operating temperature and voltages. These values are monitored, and if they exceed certain thresholds, an alert is raised so that the SFP can be scheduled for replacement before it fails.

2.3 Operating system

In this section we cover the major features of the m-type family firmware. The following features are provided in E/OS 9.0.x for devices prior to the SAN256M, and by E/OSn 6.3 or later for the SAN256M.

Tip: Many of these features are explained in more detail in *IBM TotalStorage: SAN Product, Design, and Optimization Guide*, SG24-6384.

2.3.1 Zone types and limits

Fabric zoning is the most common mechanism implemented in today's SANs to segregate the devices connected to the fabric. Zoning restricts the visibility and connectivity between devices connected to a fabric.

IBM m-type switches implement zoning by WWN or port number, or a combination of the two. This zoning is enforced at the hardware level by programming route tables in the ASICs, which prevents any frames from flowing to ports outside of their permitted zone.

Zone characteristics

The characteristics of a zone are as follows:

- Each device port that belongs to a zone is called a zone member.
- The same device can belong to more than one zone (overlapping zones).
- Zones are not restricted to single switches, but are fabric-wide.
- ISLs are not specified as zone members, only device ports.

Zone limits

Table 2-3 shows the zone limits for older and current firmware levels for the SAN256M director, the Sphereon switches, and the SAN140M director.

Table 2-3 Zone limits of old and new firmware

	<= E/OS 7.x and E/OSn 6.2.1		>= E/OS 9.0 & E/OSn 6.5	
	Other	**SAN256M**	**Other**	**SAN256M**
Unique zone member	1024	1024	4096	2048
Member per zone	1024	2048	4096	2048
Zones	1024	2048	2048	2048
Maximum devices (number of end ports)	1024	1024	1500	1500
Number of zones based on zone names with a maximum of 64 characters				

2.3.2 Element Manager

Element Manager is a licensed feature available for all switches and directors, and is accessed via the EFCM server. It provides a management GUI for an individual switch or director, and is a required feature for directors.

2.3.3 Preferred Path

This feature enables a SAN administrator to influence routing between switches or directors in a fabric. If more than one ISL connects two switches, a preference can be made for which ISL is used for a particular traffic flow.

This is done on a per switch basis by specifying the exit port (ISL) to be used for a specified target domain ID and associating it with a given entry port. For a multi-hop path, each switch or director in the route must be configured separately. See “Preferred pathing” on page 574 for how to configure a path.

2.3.4 Full Volatility

This is intended for high security environments which require that no client frame data is retained within the switch after power-off, or in data collections.

2.3.5 Open Trunking

The Open Trunking feature monitors the average data rates of all traffic flow on ISLs (from a receive port to a target domain), and periodically updates the routing tables to reroute data flow from congested links to under-utilized links, and hence efficiently use bandwidth. The objective of Open Trunking is to make the most efficient possible use of redundant ISLs between neighboring switches, even if these ISLs have different bandwidths.

Open Trunking is performed using the FSPF shortest-path routing database. This solution uses McDATA patented technology to provide real-time traffic monitoring. The feature controls Fibre Channel traffic at a flow level, rather than at a per frame level in order to achieve optimal throughput. This feature can be used on McDATA switches in homogeneous as well as heterogeneous fabrics, as it only affects traffic exiting the switch. This feature complies with current Fibre Channel ANSI standards, and operates transparently to the existing FSPF algorithms for path selection within a fabric.

There are no restrictions on which ports can be trunked together, or how many ISLs can be trunked. See “Open Trunking” on page 575 for configuring trunking.

2.3.6 N_Port ID Virtualization

This provides support for attached IBM System z9™ FCP CHPIDs to allow sharing of a physical FCP channel among OS images, whether in LPARs or as z/VM® guests. Each LPAR or guest has its own virtual N_Port, and is allocated its own unique FC address in the fabric, and hence can be zoned and LUN masked independently of other OS images sharing the physical channel. Up to 256 virtual addresses can be allocated per physical port.

2.3.7 Port fencing

Policies can be defined for E_Ports and F_Ports that block ports for misbehaving devices. They can be configured for ports which have:

- Violated security rules
- Link-level problems
- Protocol problems

This allows the user to establish policies to block ports for repeated log-in attempts that violate SANtegrity Security access configurations, devices that are experiencing “Hot I/O conditions”, and also basic protocol problems like an ISL with a faulty optic or cable that is causing the link to go up and down, triggering repeated fabric rebuilds.

2.3.8 Safe zoning mode

Safe Zoning Mode helps ensure that zone set configurations are created as expected and prevent unintended device connectivity. It also prevents a default zone from being enabled in McDATA Fabric Mode, which might lead to problems in a fabric if zones are accidentally removed or if new unzoned devices are added to the fabric.

2.3.9 Domain RSCNs

Domain register for state change notifications (domain RSCNs) are sent between end devices in a fabric to provide additional connection information to host bus adapters (HBA) and storage devices. Some HBAs might log out, then log back into the fabric when they receive an RSCN, thereby disrupting Fibre Channel traffic.

Note: This option is required if Enterprise Fabric Mode (optional SANtegrity Binding feature) is enabled.

2.3.10 Suppress RSCNs on zone set activations

Fabric format domain RSCNs are sent to ports on the switch following any change to the fabric's active zone set. These changes include activating and deactivating the zone set, or enabling and disabling the default zone. When the **Suppress RSCN's on Zone Set Activations** check box is checked, fabric format RSCNs are not sent for zone changes to attached devices.

This option is enabled by default and, in most cases, should be enabled so that attached devices can receive notification of zoning changes in the fabric. However, some HBAs might log out, then log back into the fabric when they receive an RSCN, thereby disrupting Fibre Channel traffic.

2.3.11 Logs

The following logs are available, each of which can store up to 1000 entries:

- Audit
- Event
- Hardware
- Link incident
- Threshold alert
- Security
- Open Trunking
- Advanced
  - Embedded port
  - Switch fabric

See 2.23.1, “Logs” on page 586 for more details.

2.3.12 Firmware upgrade

The EFCM server can maintain a library of firmware levels, which can be downloaded, installed and activated on a target switch or director. Code activation is transparent to SAN traffic, but might impact management applications due to loss of network connectivity.

This process is illustrated in 2.14.14, “Firmware installation” on page 478.

2.4 Management tools

Out-of-band management is provided primarily via the Ethernet network and includes:

- The EFCM family
- Telnet CLI
- SNMP for third-party applications
- SMI-S for applications such as IBM TotalStorage Productivity Center (TPC)
- Maintenance port (this is via direct RS-232 connection rather than the LAN)

In-band management is provided by the OSMS and FICON Management Server features.

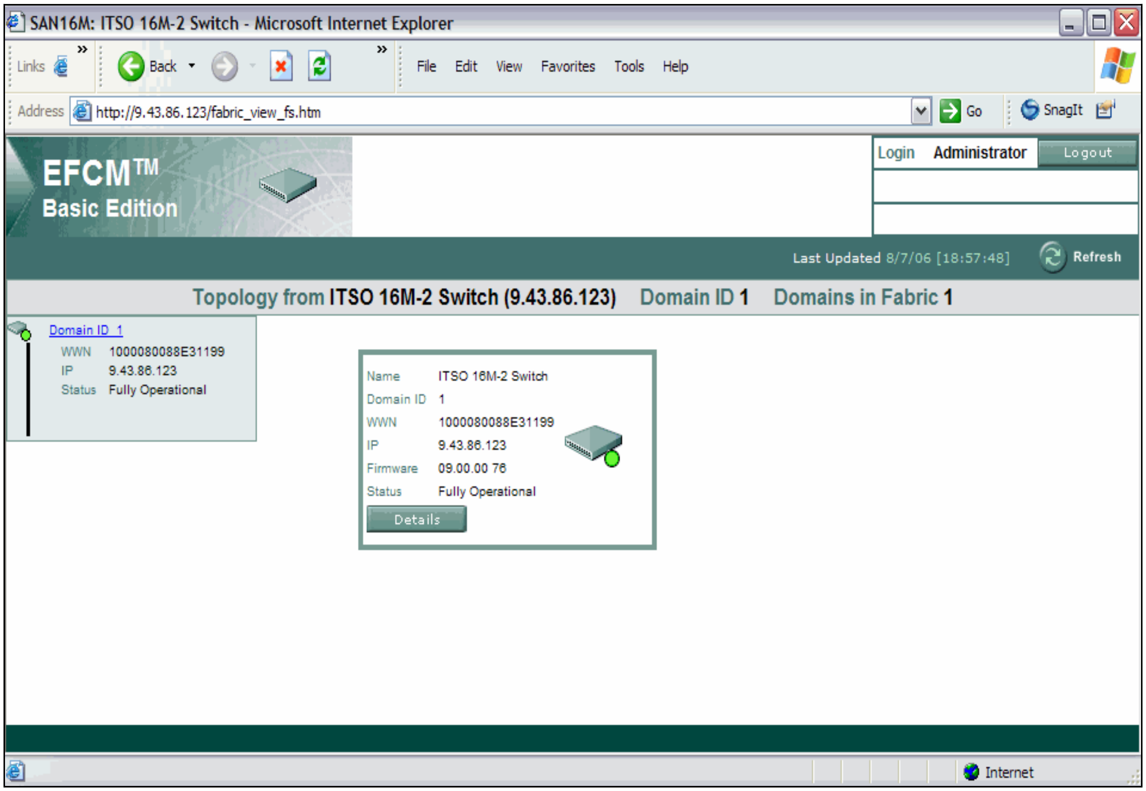
2.5 Out-of-band

All out-of-band management tools require TCP/IP network access to the switch or director. This network environment is described in 2.14.1, “Management network environment” on page 406.

2.5.1 EFCM Basic

As of E/OS 8.0, SANpilot has been re-branded as EFCM Basic, and redesigned to more closely align with the EFCM server application. It is launched by pointing a Web browser at the TCP/IP address of the switch or director, and is a standard no-charge feature on all m-type switches and directors.

Figure 2-5 shows the initial page for a SAN16M-2 switch.


SAN16M: ITSO 16M-2 Switch - Microsoft Internet Explorer
Links
Back
File
Edit
View
Favorites
Tools
Help
Address
Go
SnagIt
EFCM™
Basic Edition
Login
Logout
Refresh
Details
Internet

Address http://9.43.86.123/fabric_view_fs.htm

Login Administrator

Last Updated 8/7/06 [18:57:48]

Topology from **ITSO 16M-2 Switch (9.43.86.123)** Domain ID **1** Domains in Fabric **1**

Domain ID 1
WWN 1000080088E31199
IP 9.43.86.123
Status Fully Operational

Name ITSO 16M-2 Switch
Domain ID 1
WWN 1000080088E31199
IP 9.43.86.123
Firmware 09.00.00 76
Status Fully Operational

Figure 2-5 EFCM Basic initial page for 2026-416

Our recommendation is that, if there are three or more switches, or if you will be installing directors, then the EFCM server is required.

Enterprise Fabric Connectivity Manager is a server based management solution which runs on a client-supplied Windows server such as the IBM xSeries x306 (8836-2SU), or a Solaris server. The code is no longer ordered as a feature code against the m-type hardware, but is now a separate software product (product ID 5697-J37).

The supported server operating systems are:

- Windows 2000 Professional SP 4
- Windows 2003 Server SP 4 (enterprise recommended)
- Solaris 8 with patch cluster from 1/16/2004
- Solaris 9 with patch cluster from 1/16/2004

Shown in Table 2-4 are the minimum and recommended hardware requirements for the Windows server. As function is added in newer releases of EFCM, or the number of managed fabrics/devices increases, the minimum server requirement might also increase.

Table 2-4 EFCM server requirements for Windows

Component	Minimum	Recommended
CPU	2.0 GHz Intel® Pentium® 4	3.0 GHz 1MB/800 MHz FSB Pentium 4
Optical drive	24/8x CD-RW/DVD	48/32x CD-RW/DVD
Operating system	Windows 2000 SP 4	Windows 2003 Server Standard Edition
RAM	1 GB	2 GB DDR
Graphics Card	8MB	32 MB, VGA capable
Disk space	40 GB	40 GB ATA-100 IDE (7200 rpm)
Modem	56K, v.92 PCI modem	56K, v.92 PCI modem
Network	10/100 Mb/s Ethernet	10/100 Mb/s Ethernet

> **Note:** As of EFCM 8.0, a serial number (available from the EFCM CD jewel case) and license key are required for installation of the EFCM server.

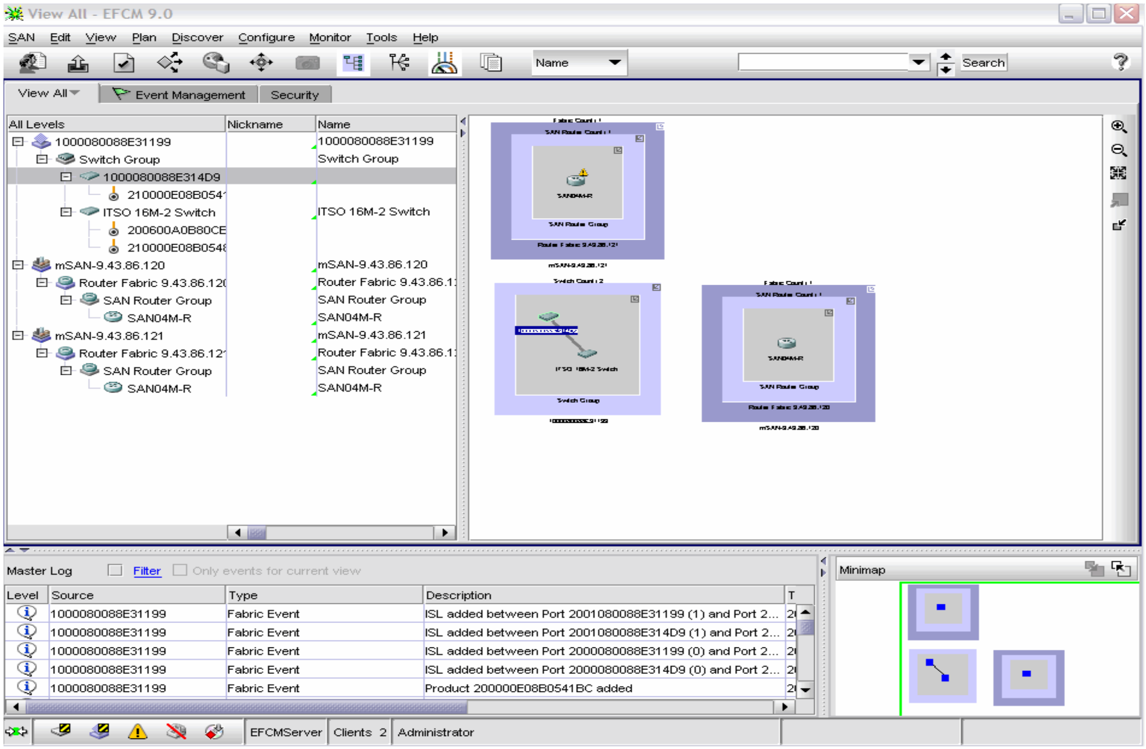
For detailed information about the EFC Manager and how to use it, refer to the *McDATA EFC Manager Software User Manual*, 620-000170. This manual can be obtained using, 2.14.13, “Obtaining software, firmware, and documentation” on page 472

Users can perform the following common product functions:

- Configure new m-type products and their associated network addresses (or product names) to the EFC Server for access through the EFC Manager and Element Manager applications.
- Display product icons that provide operational status and other information for each managed m-type product.
- Open an instance of the Element Manager application to manage and monitor a specific m-type product.
- Open the Fabrics View to display managed fabrics, manage and monitor fabric topologies, manage and monitor zones and zone sets, and show routes (data paths) between end devices attached to a multi-switch fabric.

- Define and configure user names, nicknames, passwords, SNMP agents, and user rights for access to the EFC Server, EFC Manager application, and managed m-type products, either locally or from remote user workstations.
- Configure Ethernet events, e-mail notification for system events, and call-home notification for system events.
- Display EFC audit, EFC event, session, product status, and fabric logs.

As of EFCM 8.0, the look and feel are the same as the SANavigator product, as shown in Figure 2-6. This book is written with the 9.0 version of EFCM.


View All - EFCM 9.0
SAN
Edit
View
Plan
Discover
Configure
Monitor
Tools
Help
Name
Search
View All
Event Management
Security
Master Log
Filter
Only events for current view
Minimap
EFCMServer
Clients 2
Administrator

All Levels	Nickname	Name
1000080088E31199		1000080088E31199
Switch Group		Switch Group
1000080088E314D9		
210000E08B054		
ITSO 16M-2 Switch		ITSO 16M-2 Switch
200600A0B80CE		
210000E08B054		
mSAN-9.43.86.120		mSAN-9.43.86.120
Router Fabric 9.43.86.12		Router Fabric 9.43.86.1
SAN Router Group		SAN Router Group
SAN04M-R		SAN04M-R
mSAN-9.43.86.121		mSAN-9.43.86.121
Router Fabric 9.43.86.12		Router Fabric 9.43.86.1
SAN Router Group		SAN Router Group
SAN04M-R		SAN04M-R

Level	Source	Type	Description	T
ⓘ	1000080088E31199	Fabric Event	ISL added between Port 2001080088E31199 (1) and Port 2...	2
ⓘ	1000080088E31199	Fabric Event	ISL added between Port 2001080088E314D9 (1) and Port 2...	2
ⓘ	1000080088E31199	Fabric Event	ISL added between Port 2000080088E31199 (0) and Port 2...	2
ⓘ	1000080088E31199	Fabric Event	ISL added between Port 2000080088E314D9 (0) and Port 2...	2
ⓘ	1000080088E31199	Fabric Event	Product 200000E08B0541BC added	2

Figure 2-6 EFCM 9.x main window

Optional features

EFCM has the following optional features:

Security Center

Provides simplified management of the SANtegrity Security Suite, including administration of device secrets for authentication.

Performance Monitoring and Event Management

Performance Monitoring allows you to measure the current performance statistics, historic metrics and future trends of every switch port on the SAN.

Event Management provides the ability to automate routine tasks and reduce the amount of manual intervention necessary for the management of the SAN.

Planning Manager

The tools available in the Planning Manager help evaluate the effects of a new device deployment on an existing SAN, or plan for a completely new storage network using a set of best practice configuration rules.

Group Configuration Manager

This feature can help reduce repetitive tasks by applying configuration changes to groups of devices.

> **Important:** Every device to be managed by the EFCM server must have the licensed Element Manager feature enabled.

Benefits of EFCM server

These are some of the major benefits of the EFCM server:

- Management of larger fabrics
- Management of directors as well as switches
- Automated backup of configuration data:
  - Data is backed up from directors and switches to the EFCM server:
    - Product identification data, port configuration data, and link incident (LIN) alerts
    - Operating parameters such as flow control values, preferred domain ID, Active zoning configuration and SNMP configuration
  - EFCM server data is backed up to internal CD-RW, or via a separate product such as Tivoli Storage Manager:
    - All EFC Manager configuration data such as product definitions, user definitions session options and remote event notifications
    - All log files, such as EFC Manager logs and individual director or switch Element Manager logs
    - Zoning library includes all configured zone sets and zone definitions
    - Firmware library
    - Call-home settings such as phone numbers and dialing options

  - Configuration data for each managed product, stored on the EFC Server and in NV-RAM on each director or switch
- View fabric topologies
- Fabric wide nickname support
- View consolidated fabric device status
- E-mail alerting
- Call-home support
- Managed firmware library and distribution
- Role based access controls (RBAC)

Server installation

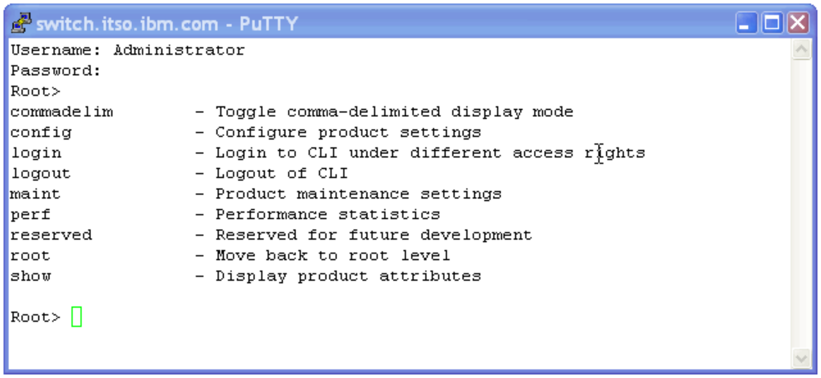
The EFCM application should be installed on a dedicated server to improve its availability and performance. It is also advisable to apply all critical Windows maintenance to the server, and to install and run an anti-virus product.

See 2.14.2, “EFCM server installation” on page 407 for an example of the server installation process.

2.5.2 CLI

Any platform that supports Telnet client software can be used for CLI access. Just start the telnet session and target default port 23 on the desired switch or director. Login with the appropriate username and password.

Figure 2-7 shows the result of logging in and entering a “?” for help.



```
Username: Administrator
Password:
Root>
commadelim          - Toggle comma-delimited display mode
config              - Configure product settings
login               - Login to CLI under different access rights
logout              - Logout of CLI
maint               - Product maintenance settings
perf                - Performance statistics
reserved            - Reserved for future development
root                - Move back to root level
show                - Display product attributes

Root>
```

Figure 2-7   Telnet CLI session after login

The CLI is normally used for scripting or debugging, whereas the GUIs are used for general management tasks. Refer to the *McDATA E/OS Command Line Interface User Manual*, 620-000134, for full details of all the commands available via the CLI. This manual can be obtained as described in 2.14.13, “Obtaining software, firmware, and documentation” on page 472.

2.5.3 SNMP

A simple network management protocol (SNMP) agent is implemented through the Element Manager application that allows administrators on SNMP management workstations to access product management information using any standard network management tool. Through the Element Manager, administrators can assign Internet Protocol (IP) addresses and corresponding community names for up to six workstations functioning as SNMP trap message recipients.

For more information, refer to the *McDATA E/OS SNMP Support Manual*, 620-000131. This manual can be obtained as described in 2.14.13, “Obtaining software, firmware, and documentation” on page 472.

2.5.4 SMI-S

The Storage Management Initiative Specification (SMI-S) is a Storage Networking Industry Association (SNIA) based standard for an interoperable management interface for multi-vendor storage networking products. McDATA provide a Common Information Model (CIM) agent for their switches and directors which enables a standard set of management functions to be performed by third-party CIM clients. It is implemented by installing the agent on a Windows or Solaris server which then talks either directly to the switch or director (Direct Connection mode), or via the EFCM server (EFCM Proxy mode).

For more information, refer to the *McDATA OPENconnectors SMI-S Interface User Guide*, 620-000210. This manual can be obtained as described in 2.14.13, “Obtaining software, firmware, and documentation” on page 472.

2.5.5 Maintenance port

An RS-232 maintenance port at the rear of the switch or director enables initial network configuration to be performed during device installation. The supplied null modem cable should be connected between the maintenance port and a laptop or desktop PC (usually the COM1 port), and terminal software such as Windows HyperTerminal used to change the default network settings. This process is shown in “Initial switch network configuration” on page 442, and requires a password to gain access.

Tip: Many modern laptops do not provide an RS-232 port. RS-232 to USB converters can be purchased, or the machine used for the EFCM server might have an RS-232 port available that can reach the maintenance port.

The maintenance port is normally only used for initial network configuration, but access might be required for problem diagnosis or problem recovery.

Attention: Provided that the switch is installed in a physically secure area, then often the default password is not changed. If the default password is changed, be certain not to lose it.

2.6 In-band

Early versions of E/OS would only support one of the following two optional features, but as of E/OS 6.0 both features can be installed. With the current release, OSMS is a standard feature.

2.6.1 Open Systems Management Server (OSMS)

OSMS is an ANSI-based feature that supports SAN management software from vendors such as IBM Tivoli. OSMS extends the switch's capability to include in-band management by an open systems host-based application. OSMS allows the fabric switch and devices attached to it to be discovered, or seen in a fabric through a framework software application

2.6.2 FICON Management Server (FMS)

The FMS is an in-band management feature developed by IBM that identifies an entity known as the Control Unit Port (CUP), which can always be accessed from any port on the switch, and is intended for zSeries host-based applications.

The following monitoring facilities are available:

- E-mail alerts from the EFCM server
- Color coded icons and status messages on the EFCM and Element Manager windows
- SNMP alerts
- Call-home by EFCM server
- Status LEDs on the hardware
- Various logs

2.7 Security

There are many aspects to SAN security, and McDATA groups all of the fabric and management related functions under the SANtegrity Security Suite banner, which covers these standard features:

- Zoning
- Role Based Access Control (RBAC)

Also, it covers these optional features:

- Binding
- Authentication
- Reporting

2.8 Zoning

This topic has already been discussed in 2.3.1, “Zone types and limits” on page 390, and is illustrated in 2.16, “Zoning” on page 531.

2.9 Role Based Access Control

Initially the EFCM server only has the `Administrator` user account defined and the following groups or roles:

- System Administrator
- Security Administrator
- Maintenance
- Operator
- Product Administrator

All groups are empty, apart from `System Administrator`, which contains the `Administrator` account.

New groups can be created, which only give access to selected features of the EFCM server, and which can be restricted to certain views. New user accounts can be created and added to one or more of the groups. This allows for the creation of user accounts in line with job responsibilities.

This process is illustrated in 2.14.7, “Defining EFCM user accounts” on page 433.

2.10 SANtegrity Binding

SANtegrity Binding enhances data security in large and complex SANs and consists of Fabric and Switch Binding features. These features provide permit and deny operations for connecting a switch to the fabric, and end device attachment to the switch or fabric. SANtegrity, and therefore the binding features, can be enabled by purchasing a feature key and then installing and activating that feature key.

2.10.1 Fabric Binding

SANtegrity Fabric Binding gives access control tools across the fabric through which the system administrator can permit or deny switches from connecting to the fabric in a SAN. Without the Fabric Binding feature enabled, the fabric/zone configuration can be easily modified or deleted by connecting a new switch to the fabric, and there are no built-in mechanisms to permit or deny any switch from merging into the fabric. It gives greater control to the system administrator and gives protection from hacking into the fabric.

After Fabric Binding is activated, a Fabric Membership List (FML) controls those switches or directors that might join the fabric. The list identifies switches by WWN and domain ID, so domain IDs must be statically allocated while Fabric Binding is active. Because of this, the Insistent Domain ID feature is automatically enabled on each switch in the fabric when Fabric Binding is activated, and it cannot be disabled while Fabric Binding is active.

See 2.17.1, “Fabric Binding” on page 555 for an example of using Fabric Binding.

2.10.2 Switch Binding

SANtegrity Switch Binding allows an administrator the option to permit/deny which end devices can be connected to director or switch ports by specifying the WWN of the devices in the Switch Membership List. Without the Switch Binding feature active on the switch, any device can connect to a switch port and there is no built-in mechanism other than Port Binding to prohibit end device connectivity. This feature provides an additional layer of security and greater access control tools for the system administrator managing complex environments that include a large number of devices.

When Switch Binding is enabled, only devices that are connected and online are identified and added to the Switch Membership List automatically. Thus the devices in the Switch Membership List are allowed to connect. Servers, storage, and other switches *not* in the Switch Membership List while Switch Binding is enabled are prohibited from connecting, and will raise alerts and attention indicators as invalid attachments.

Switch Binding has different enforcement modes:

- Restrict E_Ports
- Restrict F_Ports
- Restrict All

See “Configuring Switch Binding” on page 563 for an example of using Switch Binding.

2.11 SANtegrity Authentication

SANtegrity Authentication enables the enforcement of the requirement that each device participating in the fabric proves its identity. The process of proof is based on standards-based protocols such as FC-SP, and covers device and in-band management authentication.

2.11.1 CHAP

The Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP, or just CHAP) is used to verify device attachment.

The switch or director sends the client a random challenge value. The client must reply with a response that is the result of a cryptographic hash calculation using a shared secret. This means that both the authenticator (the switch or director) and the client must know the same client secret. Bi-directional or single direction authentication is supported, and unique secrets exist for each entity.

The switch uses CHAP to authenticate all users except Telnet and EFCM Basic users. The CHAP secrets can be held locally or in a RADIUS server.

2.11.2 RADIUS

The Remote Authentication Dial In User Service (RADIUS) is an authentication, authorization, and accounting protocol that provides applications with an external service for managing authentication. One or more RADIUS servers can be defined from which a switch or director is to obtain authentication information.

You can choose whether to use RADIUS authentication for users and/or devices independently.

Note: The RADIUS server is accessed via TCP/IP, so the LAN connection is critical to the performance of this feature.

2.12 Reporting

The EFCM Security Center provides reports of:

- Storage network configuration
- Security events
- Ports or settings that are out of policy

The Element Manager can generate an ASCII file of current configuration data. To do this, select **Configure** → **Export Configuration Report...** and specify a filename and location. The report contains:

- Product data configured in the **Configure** → **Operating Parameters** → **Identification...** dialog box
- Operating parameter data collected in the **Configure** → **Operating Parameters** dialog boxes
- Port parameters data collected in the **Configure** → **Ports...** dialog box
- SNMP parameters data collected in the **Configure** → **Operating Parameters** → **SNMP Agent...** dialog box
- Active zoning configuration, including the active zone and zone members, if set, and whether the default zone is enabled or disabled
- Alternate Control Prohibited setting that was selected from the **Configure** menu

2.13 Implementation

In this section we show examples of using the various features and management tools discussed earlier in this chapter.

2.14 Setup

First we cover those tasks that are required when installing and configuring a new EFCM server and a new switch or director.

2.14.1 Management network environment

There are two approaches to attaching m-type devices and the EFCM server to your LAN.

1. Connect all devices directly to your LAN.
2. Connect the EFCM server to your LAN using the first network port, and use a private network to connect the secondary EFCM server network port and all switches and directors. This private network can be ethernet switch or hub based.

With the first approach, it is essential that security be maintained by changing all default passwords and SNMP community strings. You should also consider whether you want to disable the CLI and Web server (EFCM Basic) interfaces on each switch if you will not be using them.

The second approach provides the benefit of isolating the fabric devices from any problems on the normal LAN. This is the approach we illustrate here in Figure 2-8.

To simplify our implementation, we assign the IP address range of 9.1.10.0/255.255.255.0 for the corporate LAN and use the 192.168.10.0 / 255.255.255.0 range for the private LAN. In this example we configure IP address 9.1.10.50 on the primary Ethernet interface for the EFC server and assign 192.168.10.1 on the secondary interface of the EFC server.

The arrows indicate the path from the remote EFC Manager client to the EFC Server. As illustrated, the m-type SAN is segregated from the corporate public network. We strongly recommended this LAN architecture to maintain high availability, manageability, fabric integrity, and optimal performance.

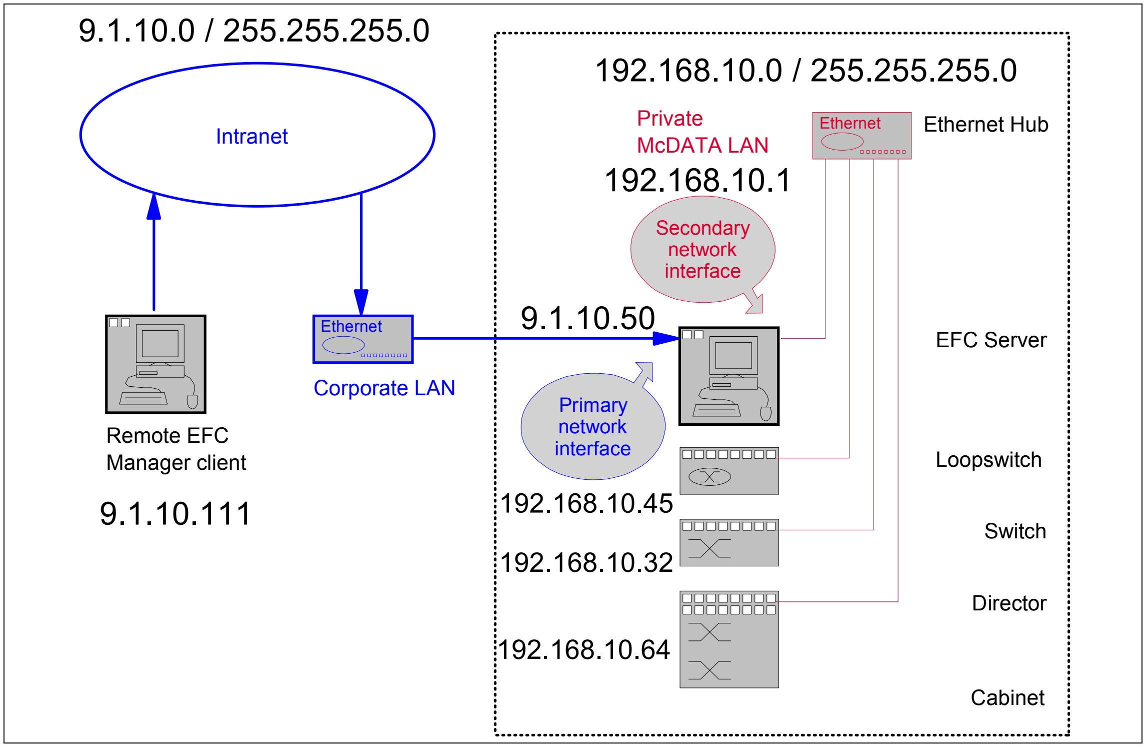

9.1.10.0 / 255.255.255.0
Intranet
Ethernet
Corporate LAN
Remote EFC Manager client
9.1.10.111
192.168.10.0 / 255.255.255.0
Private McDATA LAN
Ethernet
Ethernet Hub
192.168.10.1
Secondary network interface
9.1.10.50
EFC Server
Primary network interface
192.168.10.45
Loopswitch
192.168.10.32
Switch
Director
192.168.10.64
Cabinet

Figure 2-8 Suggested IBM TotalStorage SAN m-type family network setup

The primary ethernet interface of the EFC Server connecting to the corporate LAN can be manually configured with a valid static IP address, or configured to obtain the IP address automatically from a DHCP server. The secondary Ethernet interface must be hard configured with an IP address since we do not use a DHCP server on the private LAN. Likewise, all the fabric devices must be configured with specific IP addresses which are unique within the private LAN.

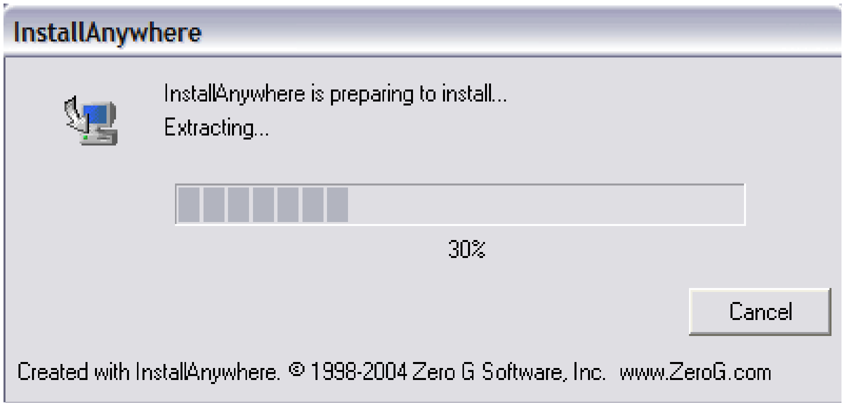
For more information on configuring the network environment, refer to the SAN Planning documentation found at the following Web site:

`http://www.mcdata.com/knowcenter/techpubs/index.html`

2.14.2 EFCM server installation

The client software is available on CD, or can be downloaded from the McDATA Web site if you are authorized (see 2.14.13, “Obtaining software, firmware, and documentation” on page 472 for details of the Web site).

The install file is over 600 MB, so if you have a slow internet link, ordering the CD might be preferable. Starting with Figure 2-9, we show the installation of the EFCM V9.0 server.



InstallAnywhere

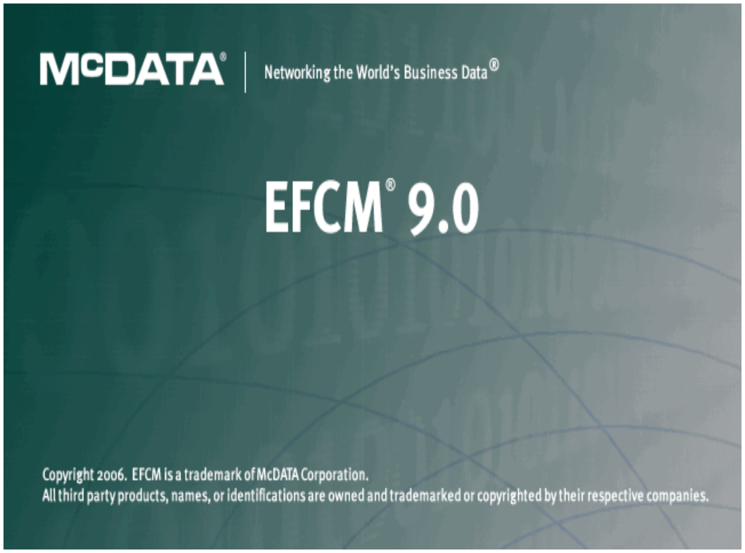
InstallAnywhere is preparing to install...
Extracting...

30%

Created with InstallAnywhere. © 1998-2004 Zero G Software, Inc. www.ZeroG.com

Figure 2-9 Extracting EFCM server code for installation

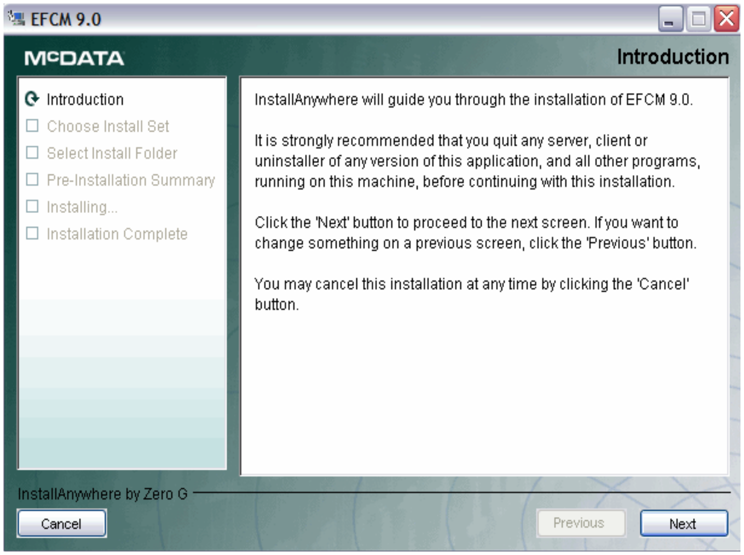
When the files have auto-extracted, the initial splash window is displayed as shown in Figure 2-10.



Copyright 2006. EFCM is a trademark of McDATA Corporation.
All third party products, names, or identifications are owned and trademarked or copyrighted by their respective companies.

Figure 2-10 EFCM server install splash window

You are then presented with the introduction window, as show in Figure 2-11, which you should read and then click **Next**.


EFCM 9.0
McDATA
Introduction
Introduction
Choose Install Set
Select Install Folder
Pre-Installation Summary
Installing...
Installation Complete
InstallAnywhere by Zero G
Cancel
Previous
Next

InstallAnywhere will guide you through the installation of EFCM 9.0.

It is strongly recommended that you quit any server, client or uninstaller of any version of this application, and all other programs, running on this machine, before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

Figure 2-11 EFCM server introduction

You are then presented with an option to select an install set, shown in Figure 2-12. You should now select the server and client option and select **Next**.

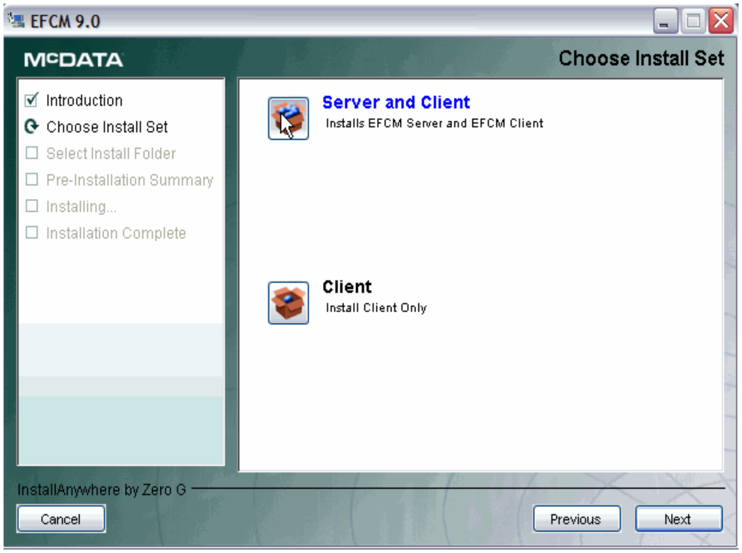
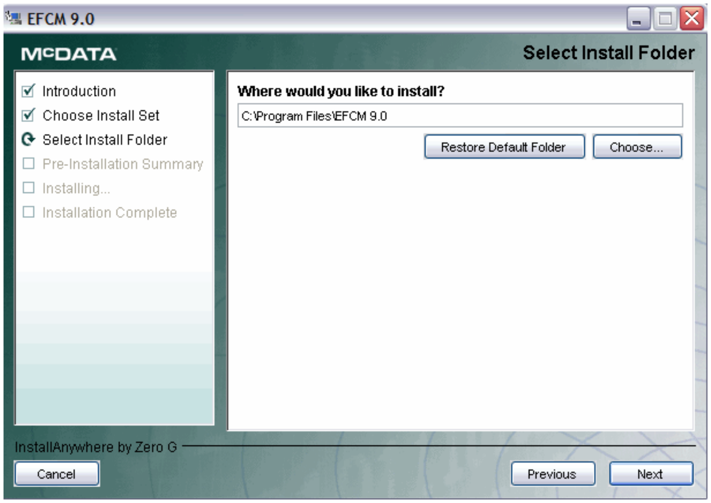

EFCM 9.0
McDATA
Choose Install Set
☑ Introduction
Choose Install Set
☐ Select Install Folder
☐ Pre-Installation Summary
☐ Installing...
☐ Installation Complete
Server and Client
Installs EFCM Server and EFCM Client
Client
Install Client Only
InstallAnywhere by Zero G
Cancel
Previous
Next

Figure 2-12 Chose install set

Figure 2-13 shows the default code installation directory. The recommendation is to use the default directory and select **Next**.

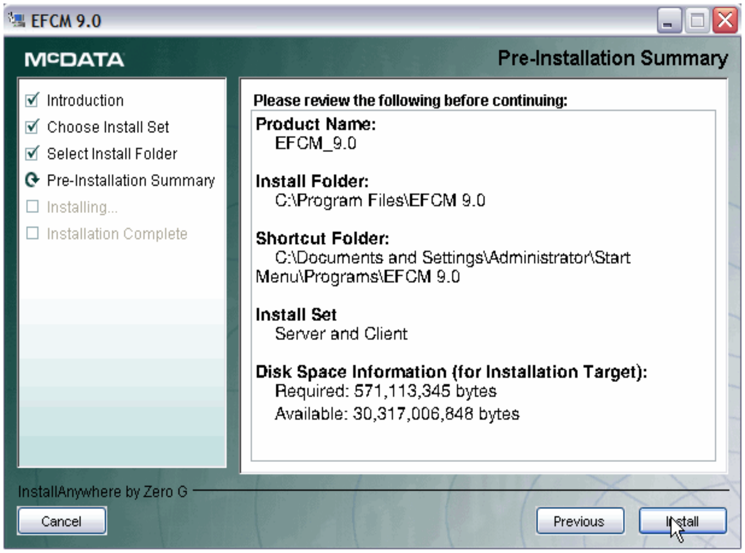

EFCM 9.0
McDATA
Select Install Folder
☑ Introduction
☑ Choose Install Set
Select Install Folder
☐ Pre-Installation Summary
☐ Installing...
☐ Installation Complete
Restore Default Folder
Choose...
InstallAnywhere by Zero G
Cancel
Previous
Next

Where would you like to install?

C:\Program Files\EFCM 9.0

Figure 2-13 EFCM server install location.

Figure 2-14 shows a summary of the pre-installation information, which you should review before clicking **Install**.


EFCM 9.0
McDATA
Pre-Installation Summary
☑ Introduction
☑ Choose Install Set
☑ Select Install Folder
Pre-Installation Summary
☐ Installing...
☐ Installation Complete
InstallAnywhere by Zero G
Cancel
Previous
Install

Please review the following before continuing:

Product Name:
EFCM_9.0

Install Folder:
C:\Program Files\EFCM 9.0

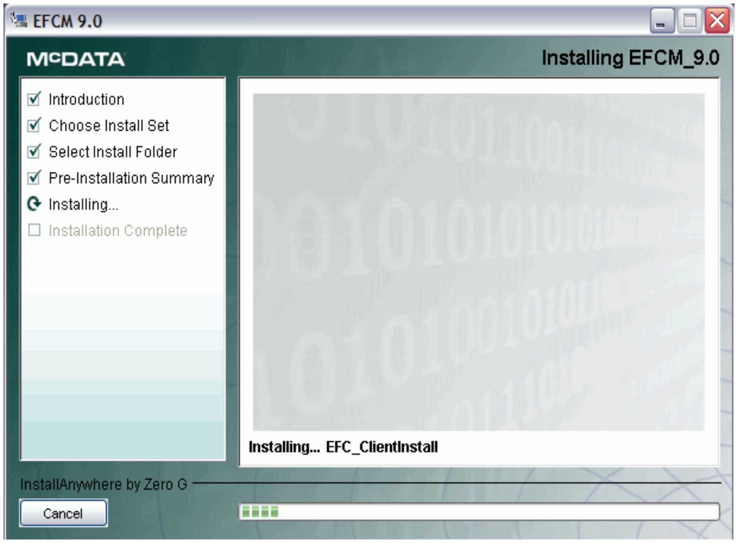
Shortcut Folder:
C:\Documents and Settings\Administrator\Start Menu\Programs\EFCM 9.0

Install Set
Server and Client

Disk Space Information (for Installation Target):
Required: 571,113,345 bytes
Available: 30,317,006,848 bytes

Figure 2-14 EFCM server pre-install summary

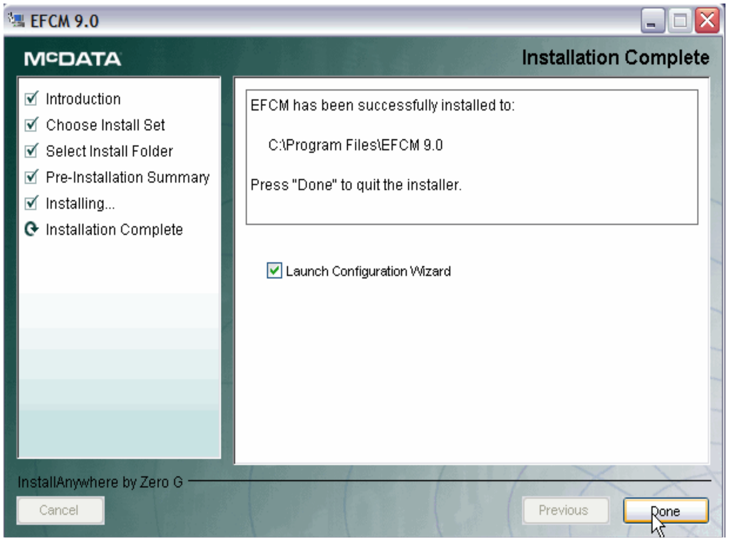
The code is now installed, as shown in Figure 2-15. This can take a few minutes.


EFCM 9.0
MCDATA
Installing EFCM_9.0
Introduction
Choose Install Set
Select Install Folder
Pre-Installation Summary
Installing...
Installation Complete
InstallAnywhere by Zero G
Cancel

Installing... EFC_ClientInstall

Figure 2-15 EFCM server code install progress

When code installation has finished, as shown in Figure 2-16, you should launch the configuration wizard by selecting the check box and **Done**.


EFCM 9.0
MCDATA
Installation Complete
Introduction
Choose Install Set
Select Install Folder
Pre-Installation Summary
Installing...
Installation Complete
InstallAnywhere by Zero G
Cancel
Previous
Done

EFCM has been successfully installed to:

C:\Program Files\EFCM 9.0

Press "Done" to quit the installer.

☑ Launch Configuration Wizard

Figure 2-16 EFCM server code install complete

You should now see the EFCM configuration welcome window as shown in Figure 2-17. Click **Next >** to proceed.

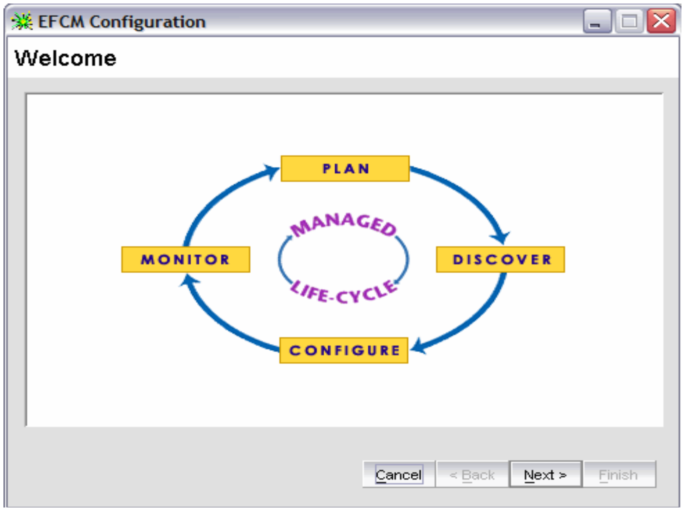
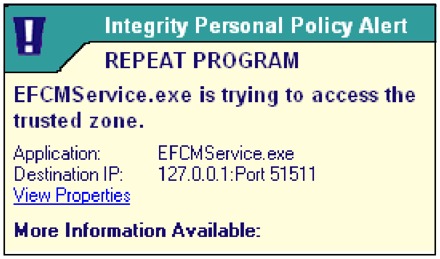

EFCM Configuration
Welcome
PLAN
DISCOVER
CONFIGURE
MONITOR
MANAGED
LIFE-CYCLE
Cancel
< Back
Next >
Finish

Figure 2-17 EFCM Configuration wizard

> **Note:** If you have a software firewall installed on the EFCM server, you might be prompted during installation to allow access to your network by the EFCMWizard.exe process as shown in Figure 2-18.


Integrity Personal Policy Alert
REPEAT PROGRAM

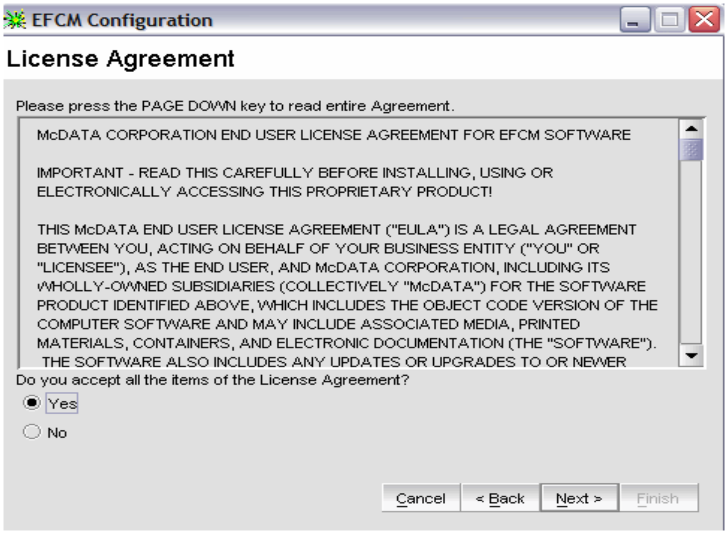
EFCMService.exe is trying to access the trusted zone.

Application: EFCMService.exe
Destination IP: 127.0.0.1:Port 51511

View Properties
More Information Available:

Figure 2-18 example of a firewall prompt during installation

Accept the license agreement by checking the **Yes** radio button, as shown in Figure 2-19, and click **Next >** to proceed.



Please press the PAGE DOWN key to read entire Agreement.

McDATA CORPORATION END USER LICENSE AGREEMENT FOR EFCM SOFTWARE

IMPORTANT - READ THIS CAREFULLY BEFORE INSTALLING, USING OR ELECTRONICALLY ACCESSING THIS PROPRIETARY PRODUCT!

THIS McDATA END USER LICENSE AGREEMENT ("EULA") IS A LEGAL AGREEMENT BETWEEN YOU, ACTING ON BEHALF OF YOUR BUSINESS ENTITY ("YOU" OR "LICENSEE"), AS THE END USER, AND McDATA CORPORATION, INCLUDING ITS WHOLLY-OWNED SUBSIDIARIES (COLLECTIVELY "McDATA") FOR THE SOFTWARE PRODUCT IDENTIFIED ABOVE, WHICH INCLUDES THE OBJECT CODE VERSION OF THE COMPUTER SOFTWARE AND MAY INCLUDE ASSOCIATED MEDIA, PRINTED MATERIALS, CONTAINERS, AND ELECTRONIC DOCUMENTATION (THE "SOFTWARE"). THE SOFTWARE ALSO INCLUDES ANY UPDATES OR UPGRADES TO OR NEWER

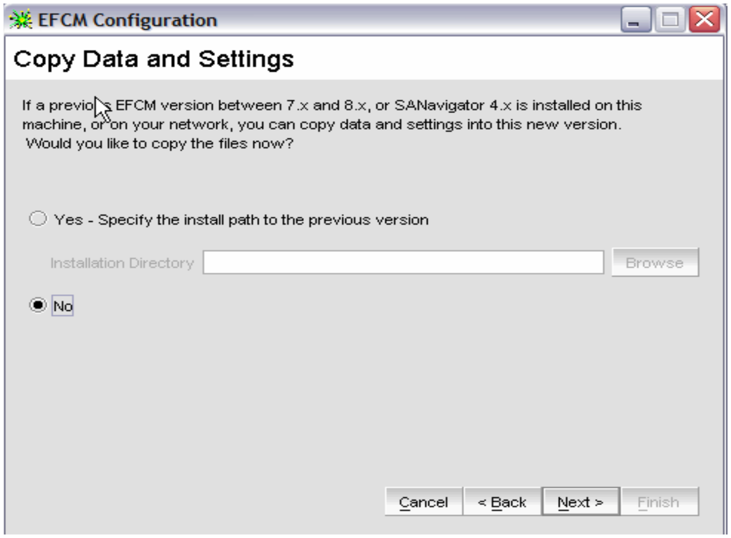
Do you accept all the items of the License Agreement?

● Yes

○ No

Figure 2-19 Accepting EFCM server license

As this is a fresh install, there are no previous settings to copy (see Figure 2-20), so select the **No** radio button and click **Next >**.



If a previous EFCM version between 7.x and 8.x, or SANavigator 4.x is installed on this machine, or on your network, you can copy data and settings into this new version. Would you like to copy the files now?

○ Yes - Specify the install path to the previous version

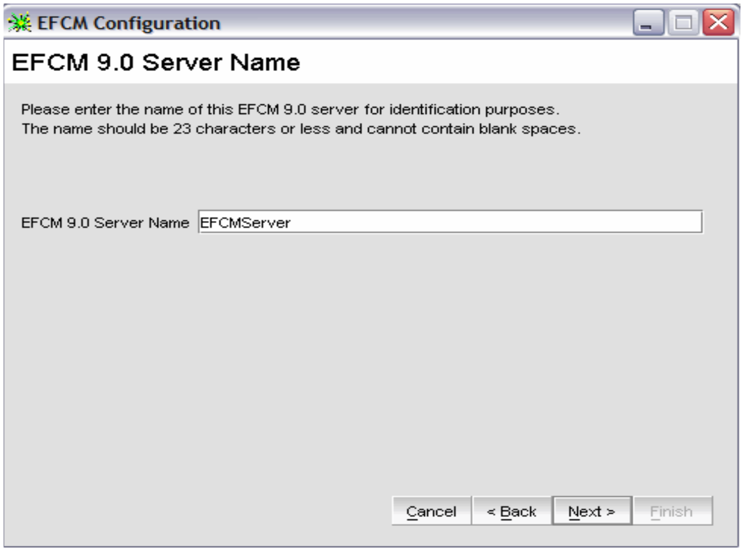
Installation Directory

● No

Figure 2-20 EFCM server fresh install

You are now given the opportunity to provide a name for your EFCM server. In the example shown in Figure 2-21, we chose `EFCMServer`. When you have entered a name, click **Next >** to proceed.

Note: The name can be no more than 20 characters long, and cannot contain any blanks.



EFCM 9.0 Server Name

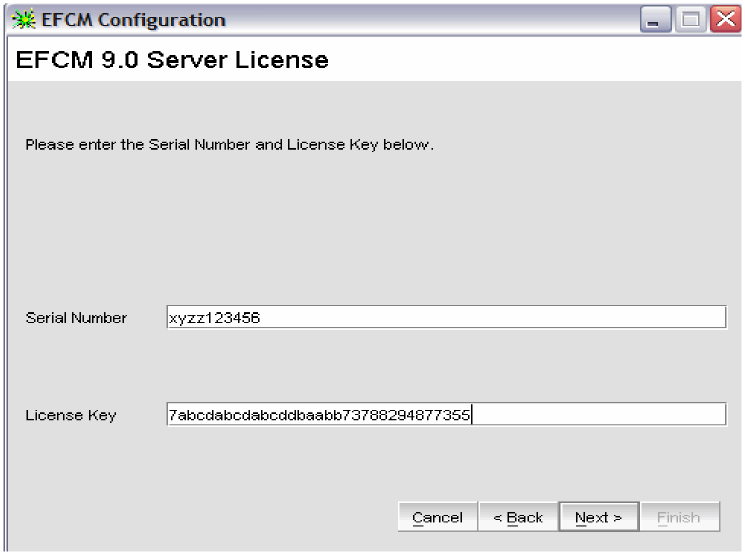
Please enter the name of this EFCM 9.0 server for identification purposes.
The name should be 23 characters or less and cannot contain blank spaces.

EFCM 9.0 Server Name: EFCMServer

Figure 2-21 Naming your EFCM server

Next you must enter your server serial number and license key. These are normally longer than those shown in Figure 2-22. When done, click **Next >** to proceed.

Tip: The EFCM serial number is available on the EFCM CD jewel case.


EFCM Configuration
EFCM 9.0 Server License

Please enter the Serial Number and License Key below.

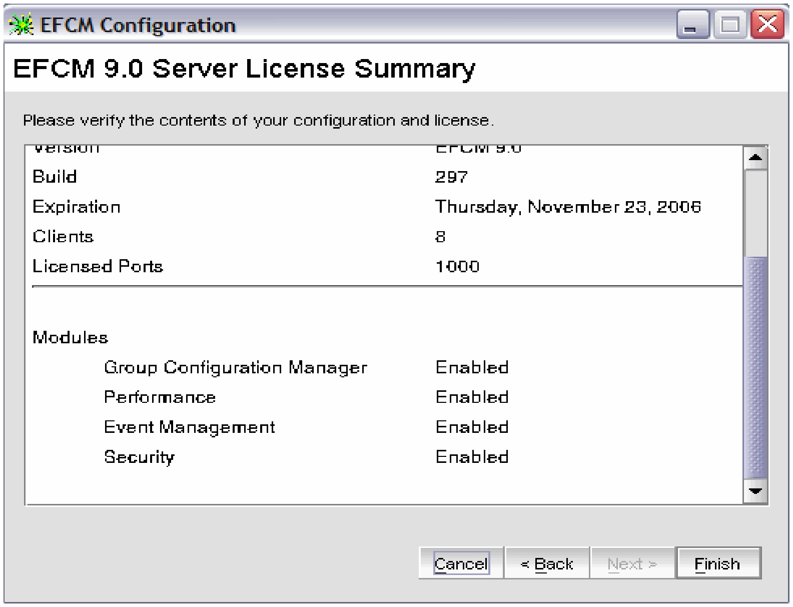
Serial Number xyzz123456

License Key 7abcdabcdabcddbaabb73788294877355

Cancel
< Back
Next >
Finish

Figure 2-22 EFCM server key and license

You have reached the end of the initial EFCM server configuration, and you are now shown a summary of your installation as well as a list of modules that have been enabled by your licence key, as shown in Figure 2-23. Click **Finish**.



EFCM 9.0 Server License Summary

Please verify the contents of your configuration and license.

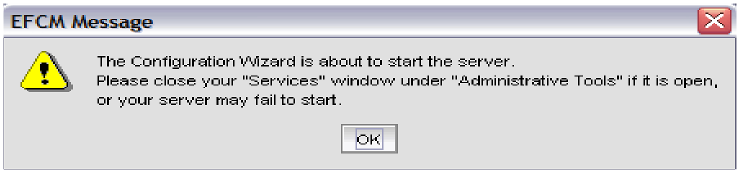
Version	EFCM 9.0
Build	297
Expiration	Thursday, November 23, 2006
Clients	8
Licensed Ports	1000

Modules

Group Configuration Manager	Enabled
Performance	Enabled
Event Management	Enabled
Security	Enabled

Figure 2-23   EFCM server initial configuration complete

Respond to the message shown in Figure 2-24 by clicking **OK** to start the server.



The Configuration Wizard is about to start the server.
Please close your "Services" window under "Administrative Tools" if it is open,
or your server may fail to start.

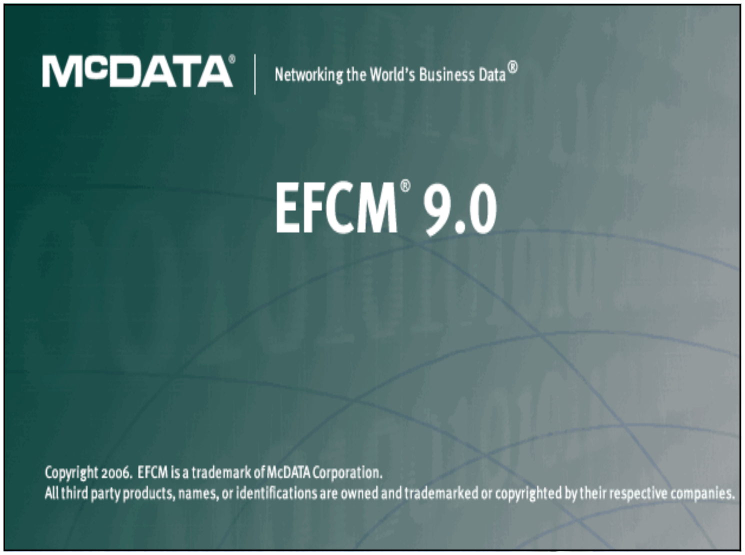
Figure 2-24   Starting EFCM server the first time

Note: If you have a software firewall installed on the EFCM server, you might be prompted during server initialization to allow access to your network by the EFCMService.exe and the EFCMClient.exe processes as shown in Figure 2-18 on page 412.

EFCM Server installation is now complete, and you should proceed to initial server configuration.

2.14.3 EFCM server initial configuration

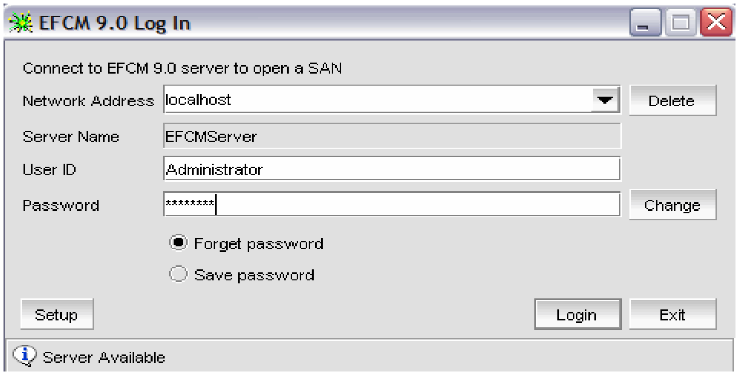
When the server has started, the EFCM client automatically starts, as shown by the splash window in Figure 2-25.


McDATA®
Networking the World's Business Data®
EFCM® 9.0

Copyright 2006. EFCM is a trademark of McDATA Corporation.
All third party products, names, or identifications are owned and trademarked or copyrighted by their respective companies.

Figure 2-25 EFCM client splash window

When the client has started, you are prompted with the log in panel shown in Figure 2-26. The initial user ID is `Administrator`, and the default password is `password` (both are case sensitive). Click **Login**.


EFCM 9.0 Log In
Delete
Change
Setup
Login
Exit

Connect to EFCM 9.0 server to open a SAN

Network Address: localhost

Server Name: EFCMServer

User ID: Administrator

Password: ********

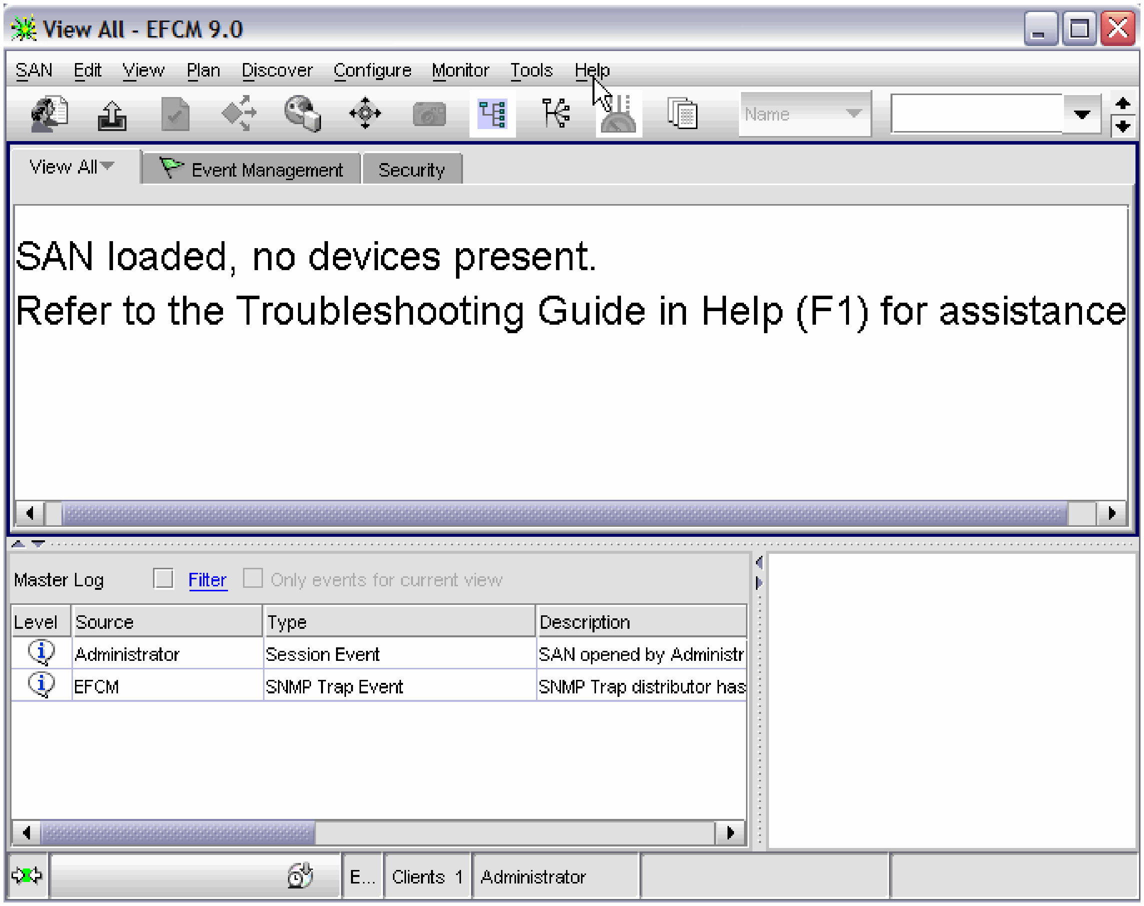
● Forget password

○ Save password

Server Available

Figure 2-26 EFCM client log in window

You should see the main EFCM server window, as shown in Figure 2-27.


View All - EFCM 9.0
SAN Edit View Plan Discover Configure Monitor Tools Help
Name
View All
Event Management
Security
Master Log
Filter
Only events for current view
E...
Clients 1
Administrator

SAN loaded, no devices present.
Refer to the Troubleshooting Guide in Help (F1) for assistance

Level	Source	Type	Description
ⓘ	Administrator	Session Event	SAN opened by Administr
ⓘ	EFCM	SNMP Trap Event	SNMP Trap distributor has

Figure 2-27 EFCM main window

You are now ready to discover your fabric and use the EFCM server locally.

> **Important:** If you plan on accessing the EFC Server through a firewall, some manual editing of the EFC Server configuration might be required, as described in 2.14.6, “Firewall considerations” on page 429.

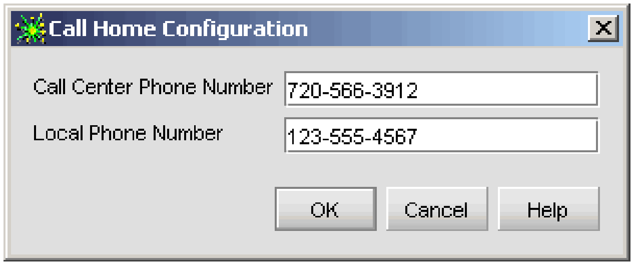
Server call home

Connect the EFCM server modem to the telephone line, then double-click the *Call Home Configuration* icon, shown in Figure 2-28.

Call Home
Configuration

Figure 2-28 Call Home desktop icon

Enter the telephone number of the support center, and the telephone number of the local line, as shown in Figure 2-29, and click **OK**.

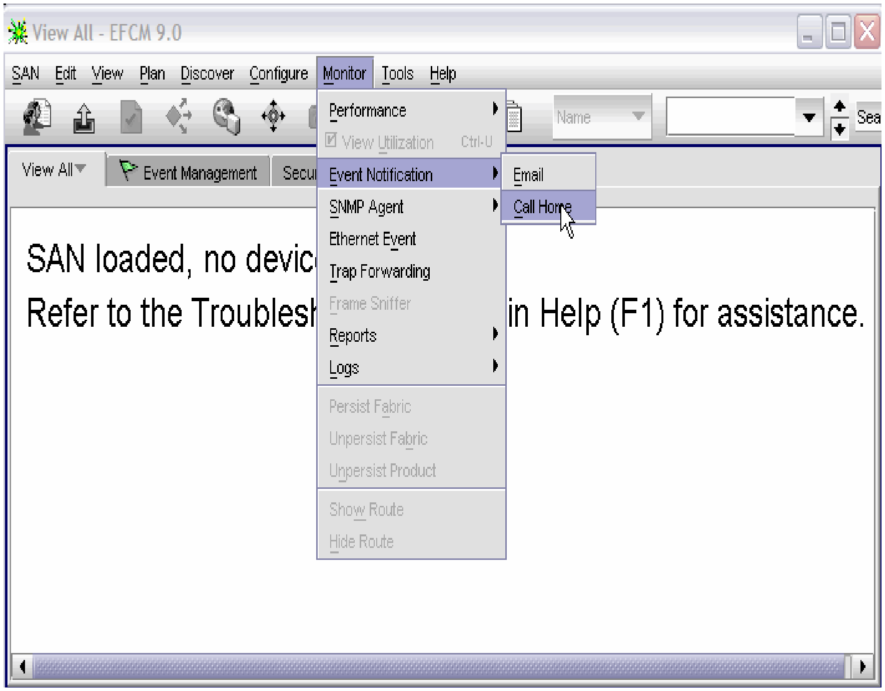

Call Home Configuration
OK
Cancel
Help

Call Center Phone Number 720-566-3912

Local Phone Number 123-555-4567

Figure 2-29 Call Home example telephone numbers

Now select **Monitor** → **Event Notification** → **Call Home** and ensure that the **Enable Call Home Event Notification** check box is checked (see Figure 2-30.

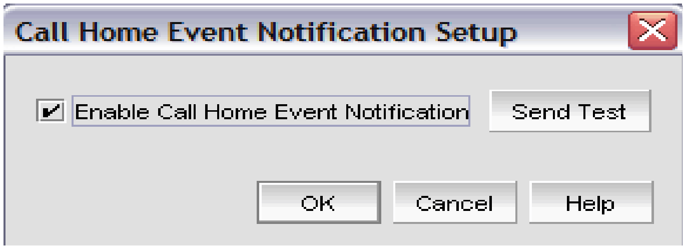

View All - EFCM 9.0
SAN
Edit
View
Plan
Discover
Configure
Monitor
Tools
Help
Name
Sea
View All
Event Management
Secu
Performance
View Utilization Ctrl-U
Event Notification
SNMP Agent
Ethernet Event
Trap Forwarding
Frame Sniffer
Reports
Logs
Persist Fabric
Unpersist Fabric
Unpersist Product
Show Route
Hide Route
Email
Call Home

SAN loaded, no devic

Refer to the Troublesh in Help (F1) for assistance.

Figure 2-30 Call home setup and test selection

You can use this option also to perform a test of the call home function, as shown in Figure 2-30 and Figure 2-31.


Call Home Event Notification Setup
Send Test
OK
Cancel
Help

☑ Enable Call Home Event Notification

Figure 2-31 Call home setup and test

More details on this procedure are available in *EFC Manager Software User Manual*, 620-000170.

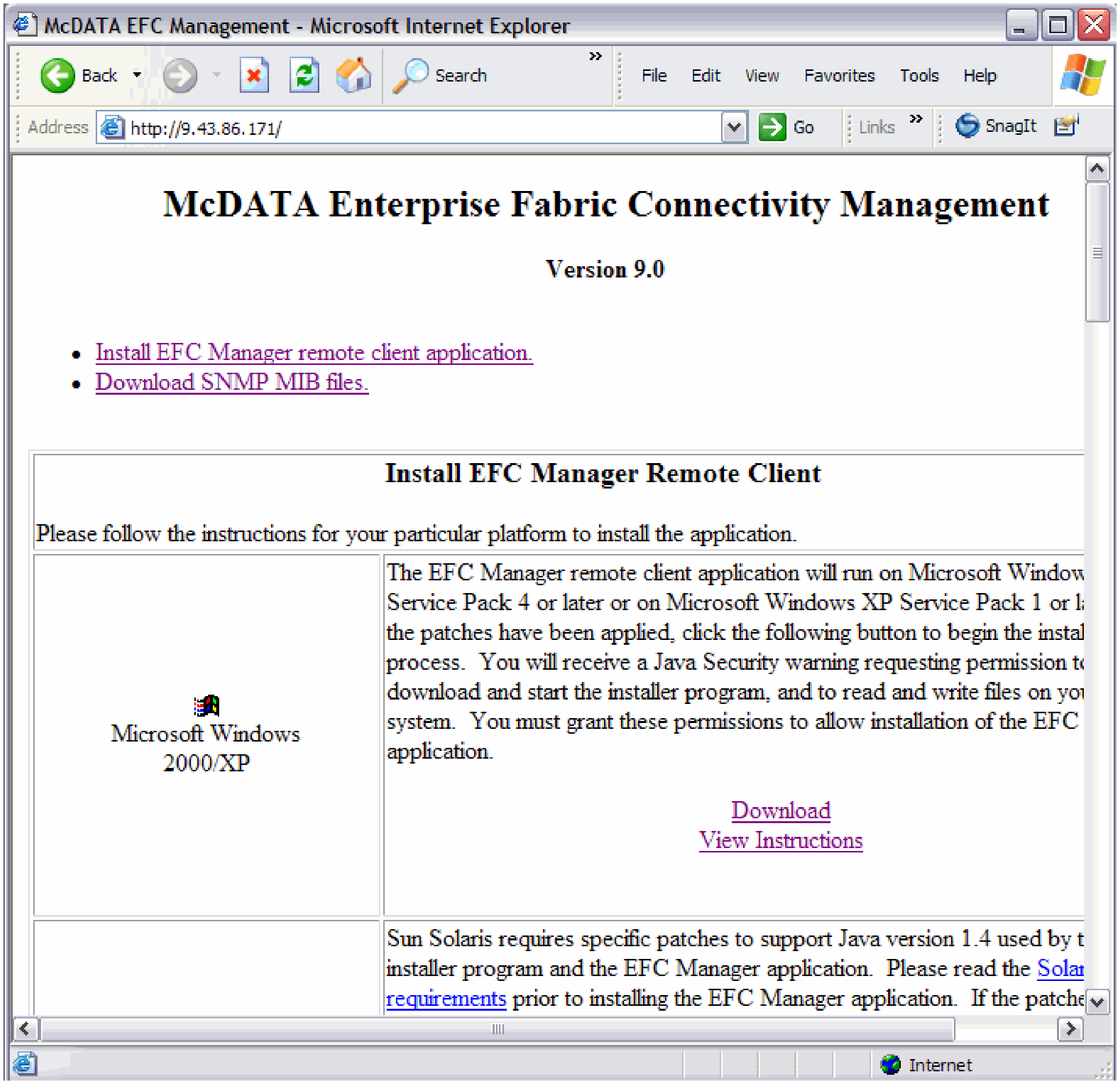
2.14.4 EFCM remote client installation

EFCM clients are available for the following platforms:

- Windows 2003
- Windows 2000 with service pack 3 or higher
- Windows XP Professional with Service pack 2
- AIX 5.1 ML 4
- HP/UX 11.00
- Linux Red Hat 9
- Sun Solaris SPARC 8.0, 9.0, and 10.0

The client software is available on CD, or can be downloaded from a Web server on the EFCM server, and installed on a client workstation. It is also possible to download SNMP MIB files from the Web server.

Target your browser at the TCP/IP address or hostname of your EFCM server as shown in Figure 2-32.


McDATA EFC Management - Microsoft Internet Explorer
Back
Search
File
Edit
View
Favorites
Tools
Help
Address
http://9.43.86.171/
Go
Links
SnagIt
Internet

McDATA Enterprise Fabric Connectivity Management

Version 9.0

- Install EFC Manager remote client application.
- Download SNMP MIB files.

Install EFC Manager Remote Client

Please follow the instructions for your particular platform to install the application.

Microsoft Windows 2000/XP

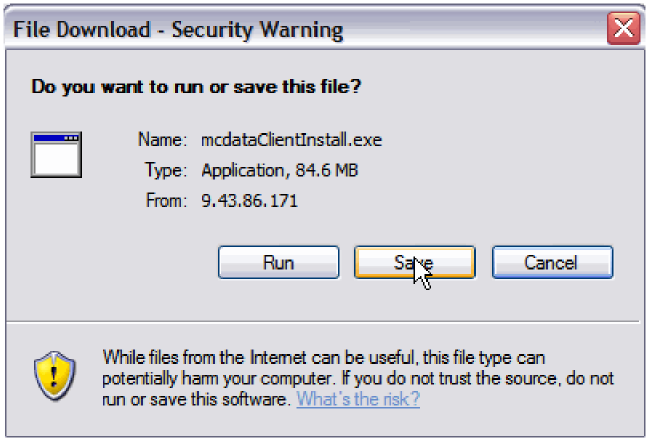
The EFC Manager remote client application will run on Microsoft Window Service Pack 4 or later or on Microsoft Windows XP Service Pack 1 or l the patches have been applied, click the following button to begin the instal process. You will receive a Java Security warning requesting permission t download and start the installer program, and to read and write files on you system. You must grant these permissions to allow installation of the EFC application.

Download
View Instructions

Sun Solaris requires specific patches to support Java version 1.4 used by t installer program and the EFC Manager application. Please read the Sola requirements prior to installing the EFC Manager application. If the patche

Figure 2-32 Start page for remote EFC Manager client installation download

We are installing on Windows, so we click the first **Download** link and save the file to disk as shown in Figure 2-33.



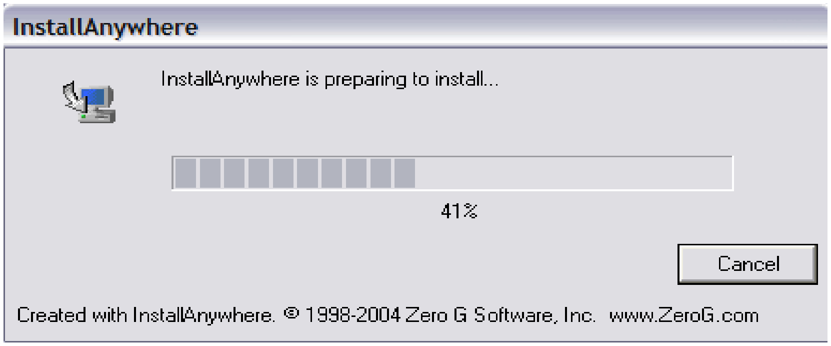
Do you want to run or save this file?

Name: mcdataClientInstall.exe
Type: Application, 84.6 MB
From: 9.43.86.171

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Figure 2-33 Client download dialogue

When the file is saved, browse to the directory where you saved the file and launch the **`mcdataClientInstall.exe`** file, you then see the file extraction window shown in Figure 2-34.

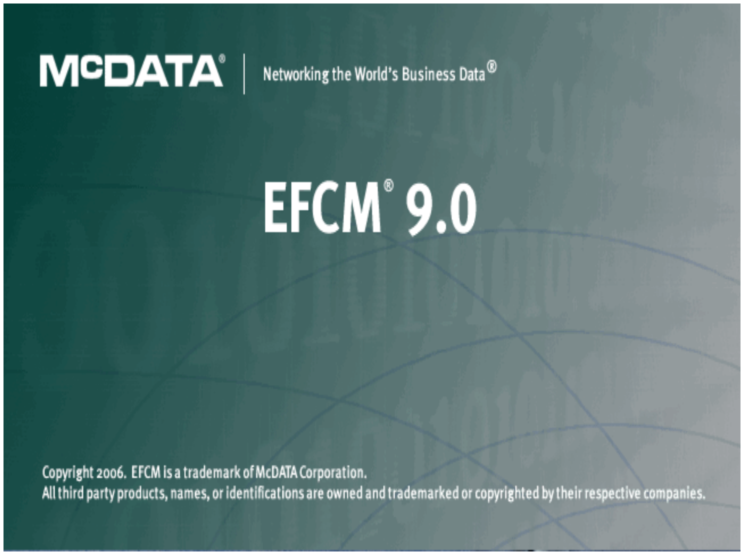


InstallAnywhere is preparing to install...

Created with InstallAnywhere. © 1998-2004 Zero G Software, Inc. www.ZeroG.com

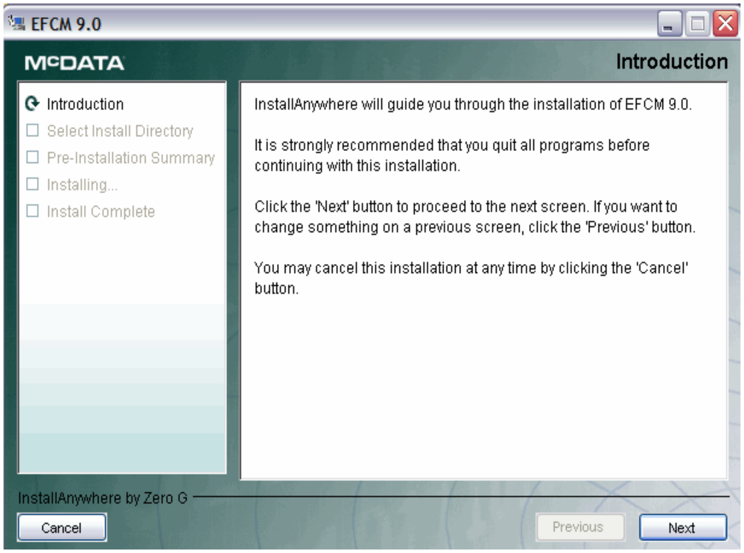
Figure 2-34 Extracting EFCM client code for installation

As shown in Figure 2-35, the splash window is displayed. This is replaced by the introduction window shown in Figure 2-36.


McDATA
Networking the World's Business Data®
EFCM® 9.0

Copyright 2006. EFCM is a trademark of McDATA Corporation.
All third party products, names, or identifications are owned and trademarked or copyrighted by their respective companies.

Figure 2-35 EFCM client install splash window


EFCM 9.0
McDATA
Introduction
Introduction
Select Install Directory
Pre-Installation Summary
Installing...
Install Complete
InstallAnywhere by Zero G
Cancel
Previous
Next

InstallAnywhere will guide you through the installation of EFCM 9.0.

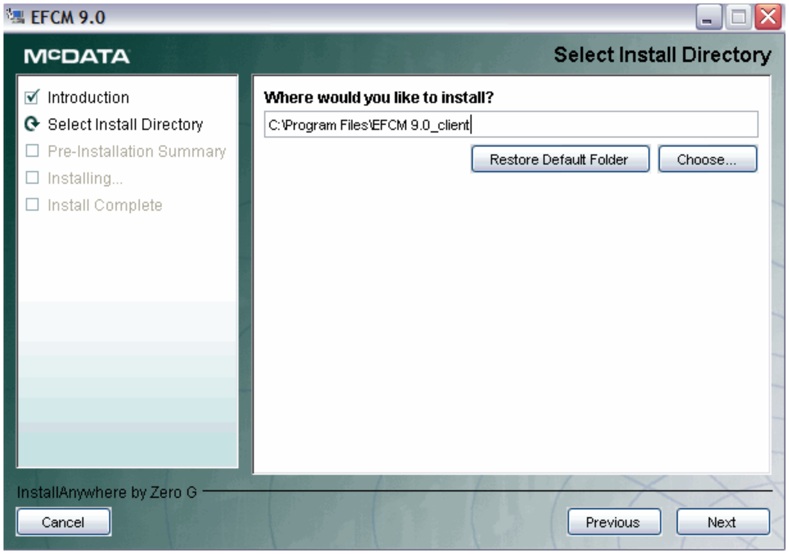
It is strongly recommended that you quit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

Figure 2-36 EFCM client install introduction

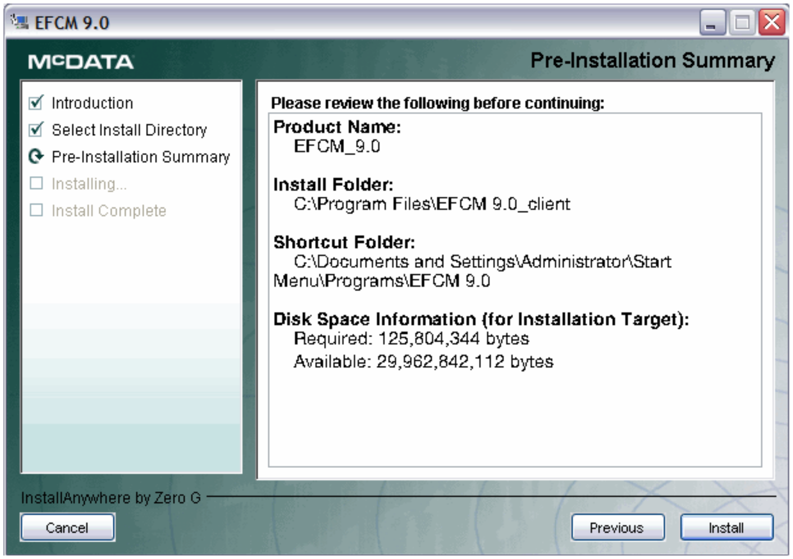
Click **Next** to be presented with the choice of where to install the client. Figure 2-37 shows the default code installation directory. Modify this if required and click **Next**.


EFCM 9.0
McDATA
Select Install Directory
☑ Introduction
Select Install Directory
☐ Pre-Installation Summary
☐ Installing...
☐ Install Complete
Restore Default Folder
Choose...
InstallAnywhere by Zero G
Cancel
Previous
Next

Where would you like to install?
C:\Program Files\EFCM 9.0_client

Figure 2-37 EFCM client install location

Figure 2-38 show a summary of the pre-installation information, which you should review before clicking **Install**.


EFCM 9.0
McDATA
Pre-Installation Summary
☑ Introduction
☑ Select Install Directory
Pre-Installation Summary
☐ Installing...
☐ Install Complete
InstallAnywhere by Zero G
Cancel
Previous
Install

Please review the following before continuing:

Product Name:
EFCM_9.0

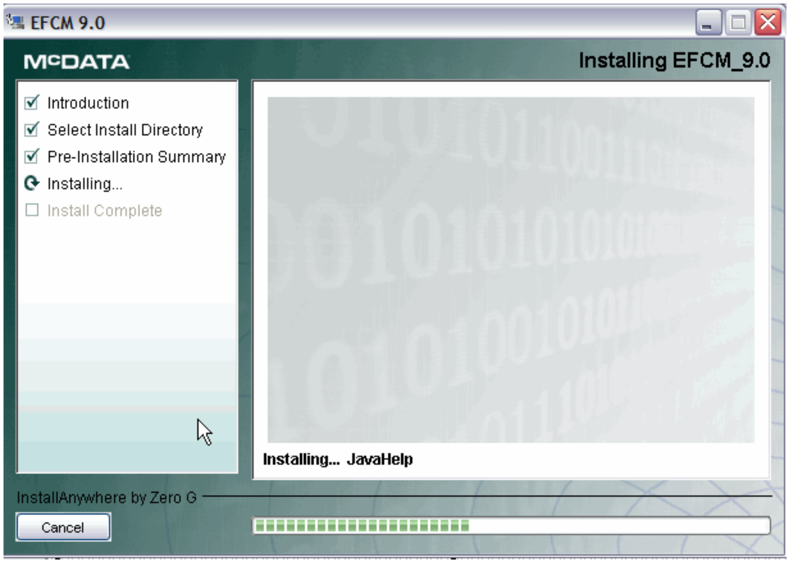
Install Folder:
C:\Program Files\EFCM 9.0_client

Shortcut Folder:
C:\Documents and Settings\Administrator\Start Menu\Programs\EFCM 9.0

Disk Space Information (for Installation Target):
Required: 125,804,344 bytes
Available: 29,962,842,112 bytes

Figure 2-38 EFCM client pre-install summary

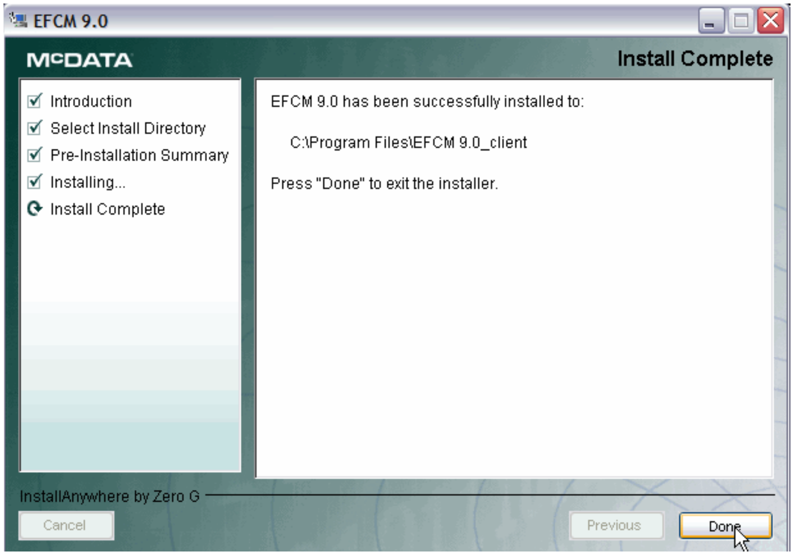
The code is now installed, as shown in Figure 2-39.


EFCM 9.0
MCDATA
Installing EFCM_9.0
☑ Introduction
☑ Select Install Directory
☑ Pre-Installation Summary
Installing...
☐ Install Complete
InstallAnywhere by Zero G
Cancel

Installing... JavaHelp

Figure 2-39 EFCM client code install progress

When code installation has finished, as shown in Figure 2-40, you should exit the installer by clicking **Done**.


EFCM 9.0
MCDATA
Install Complete
☑ Introduction
☑ Select Install Directory
☑ Pre-Installation Summary
☑ Installing...
Install Complete
InstallAnywhere by Zero G
Cancel
Previous
Done

EFCM 9.0 has been successfully installed to:

C:\Program Files\EFCM 9.0_client

Press "Done" to exit the installer.

Figure 2-40 EFCM client code install complete

You should now have the EFCM client icon on your desktop, as shown in Figure 2-41.

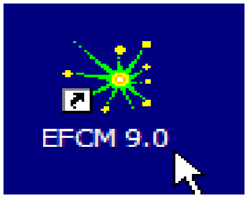


Figure 2-41 EFCM client desktop icon

2.14.5 Starting the remote EFCM client

Double-click the icon, as shown in Figure 2-41, to launch the EFCM client application.

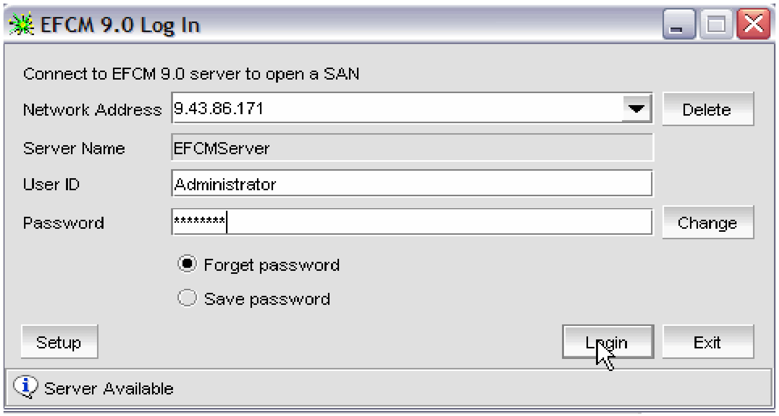
The splash window shown in Figure 2-42 displays briefly.

McDATA®
Networking the World's Business Data®
EFCM® 9.0

Copyright 2006. EFCM is a trademark of McDATA Corporation.
All third party products, names, or identifications are owned and trademarked or copyrighted by their respective companies.

Figure 2-42 EFCM client splash window

You now get the login window, as shown in Figure 2-43.



Connect to EFCM 9.0 server to open a SAN

Network Address: 9.43.86.171
Server Name: EFCMServer
User ID: Administrator
Password: ********

● Forget password
○ Save password

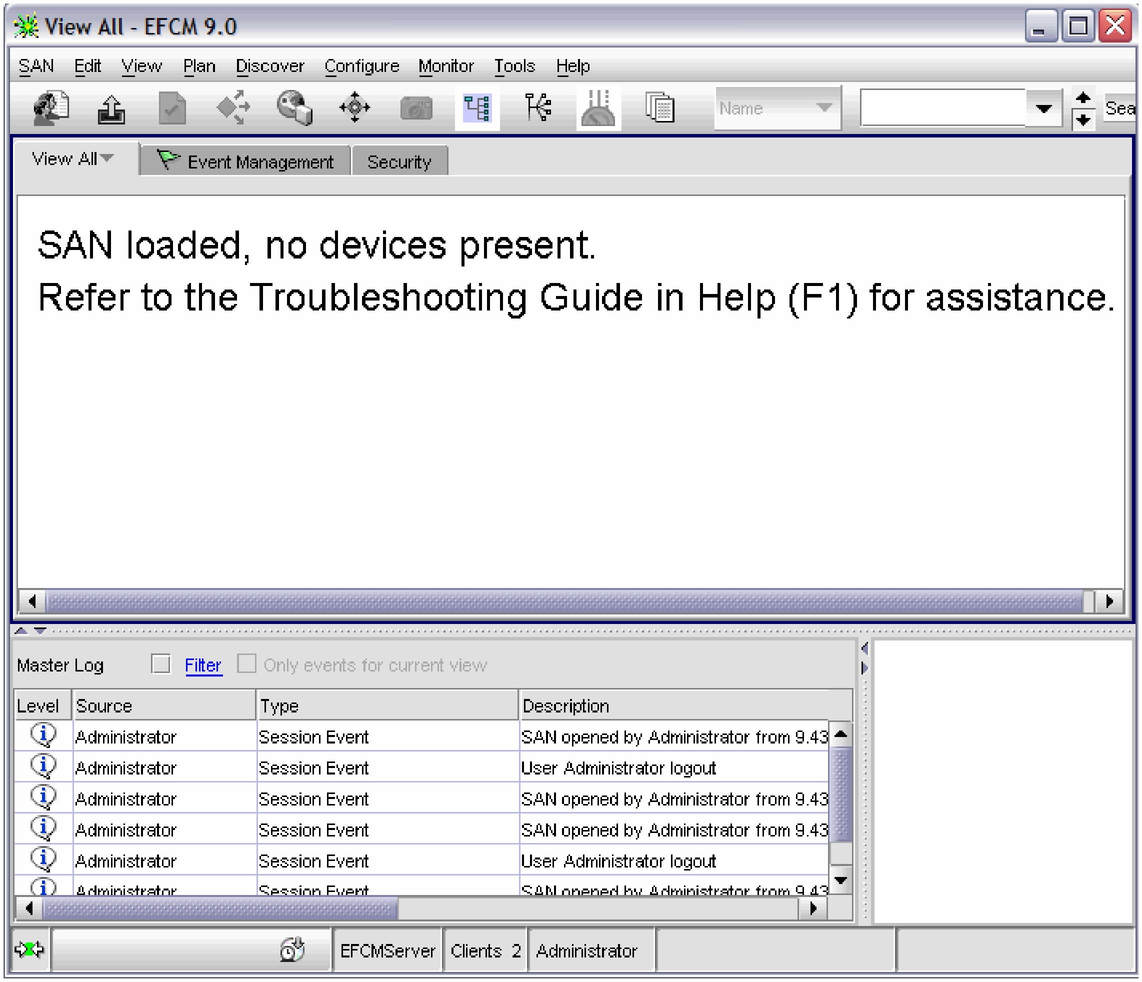
Server Available

Figure 2-43 EFCM client log in panel

> **Important:** See 2.14.6, "Firewall considerations" on page 429 if there is a hardware firewall between the client and the server.

The initial user ID is `Administrator`, and the default password is `password` (both are case sensitive). When you click **Login**, the `Server Available` message at the bottom of the window should change to `Logging In`, which can take a while.

You have to use the network address of the EFCM server. The main EFCM server window is now displayed, as shown in Figure 2-44.


View All - EFCM 9.0
SAN Edit View Plan Discover Configure Monitor Tools Help
Name
Sea
View All
Event Management
Security
Master Log
☐ Filter
☐ Only events for current view
EFCMServer
Clients 2
Administrator

SAN loaded, no devices present.
Refer to the Troubleshooting Guide in Help (F1) for assistance.

Level	Source	Type	Description
ⓘ	Administrator	Session Event	SAN opened by Administrator from 9.43
ⓘ	Administrator	Session Event	User Administrator logout
ⓘ	Administrator	Session Event	SAN opened by Administrator from 9.43
ⓘ	Administrator	Session Event	SAN opened by Administrator from 9.43
ⓘ	Administrator	Session Event	User Administrator logout
ⓘ	Administrator	Session Event	SAN opened by Administrator from 9.43

Figure 2-44 EFCM client main window

You are now ready to use the EFCM server remotely.

2.14.6 Firewall considerations

If there is a firewall between the EFCM server and its clients, or between the EFCM server and the managed products, then some configuration updates are required to enable communication. Notice that all text in the configuration files is case sensitive.

EFCM client to server access

Starting with EFCM V8.5, SSL is used to encrypt application traffic between the client and server. Two ports are used by default for this communication:

- 50511 is unencrypted and is used for the initial connection and to look up the version compatibility between the client and server.
- 50510 is encrypted and used for all application traffic, once connected.

Additionally, port 51512 is used by default for Telnet CLI proxy access to managed devices through the EFCM server if the managed devices are on a private LAN behind the EFCM server.

> **Important:** The server fails to initialize if any of its required ports are unavailable. In addition to the three ports mentioned above, the default port for ECCAPI communication is 51513.

Modifying EFCM configuration files

The server configuration file is called:

`C:\Program Files\EFCM x.y\resources\Server\config.properties`

The client configuration file is called:

`C:\Program Files\EFCM x.y Client\resources\Client\config.properties`

When editing the files, remember the following considerations:

- Make a backup copy of the file you are about to change.
- In both cases, *x.y* corresponds to the installed version, which would be 9.0 for the current version.
- The client file should already exist, but might be empty.
- A # preceding the line disables (comments out) the parameter. Remove the # to enable the parameter change.
- The contents of the files are case sensitive.
- Any errors in the configuration file cause the client to fail to start.

> **Important:** Remember to re-apply any changes if you upgrade or re-install your EFCM software.

Default ports with duplex access

If you can allow duplex traffic through your firewall for the default ports, then further configuration of EFCM is not required.

Default ports without duplex access

If you cannot allow duplex traffic, but can allow the default ports, then client access will work with the default configuration, but the initial client login step will be slower than normal. See “Slow client logins” on page 433 for suggestions on how to improve initial login performance.

Changing default ports — two port access

If the default port values cannot be used, then they can be changed. This requires updating both the server and client configuration files.

If we had to change the initial connection port from 51511 to 3001 and the application data port from 51510 to 3000, we would make the following changes:

1. Edit the configuration file on the server and uncomment the lines shown and change the values:

   ```
   # Most Secure setup for use through a firewall.
   # Two Ports must be opened, one for the RMI registry lookup and one for the
   SSL data connections.
   smp.registry.port=3001
   smp.server.export.port=3000
   ```

   Remember to restart the EFCM Service.

2. Edit the configuration file on the client and add the line shown:

   ```
   smp.registry.port=3001
   ```

Note: The client registry port must match that defined on the server.

Changing default ports — single port access

If you can only enable one port through your firewall, then you must disable encryption, because the SSL and registry connections cannot coexist on a single port. This requires updating both the server and client configuration files.

If we had to change the initial connection port and the application data port to both be 4000, we would make the following changes:

1. Edit the configuration file on the server and uncomment the lines shown and change the values:

   ```
   # Secure setup for use through a firewall with only one port open. Note
   that SSL connections and RMI registry
   # connections cannot coexist on a single port thus SSL must be disabled.
   smp.ssl=false
   smp.registry.port=4000
   smp.server.export.port=4000
   ```

   Remember to restart the EFCM Service.

2. Edit the configuration file on the client and add the line shown:

```
smp.registry.port=4000
```

Note: The client registry port must match that defined on the server.

Client call-back port

The client port used to receive updates pushed from the server is allowed to roam. If you have to fix this for remote clients, then it is best to set it to the same port as the smp.server.export.port.

Edit the configuration file on the client, add the line shown, and change the value:

```
smp.client.export.port=51510
```

Restriction: Do not do this for the local client on the EFCM server.

Changing CLI proxy port

If you want to change the default port used for the CLI proxy, edit the configuration file on the server, uncomment the line shown, and change the value (in this case we picked 5023):

```
# The port number the CliProxy listens on. The usual telnet default is 23. EFCM
default is 51512.
smp.server.cliProxyListeningPort=5023
```

Remember to restart the EFCM Service.

Changing ECCAPI port

If you want to change the default port, edit the configuration file on the server, uncomment the line shown, and change the value:

```
# The ECC API's remote object will be exported on this port. Default = 51513
smp.server.ecc.api.export.port=51513
```

Remember to restart the EFCM Service.

Disabling encryption

The overhead of encryption is negligible and it should normally be left enabled, but if you want to disable it, edit the configuration file on the server and uncomment the line shown:

```
# Port and Secure Socket Layer (SSL) Configuration
# SSL is enabled by default on the connections between the client and server.
smp.ssl=false
```

Remember to restart the EFCM Service.

Network firewall

On the network firewall between the EFCM client and the EFCM server, configure the firewall to allow your chosen ports through; remember to allow bi-directional access if possible.

The EFCM server connects to port 2048 on managed devices (switches), so if the firewall is in between, configure it to allow traffic on TCP/IP port 2048.

EFCM also uses FTP between the client and the server, so the firewall administrator must allow the well-known FTP port 21 through as well.

Slow client logins

In normal operation, the EFCM server pushes updates to the client when they occur. If duplex access is not available, the EFCM client switches to “polling mode”, where it checks with the server every 5 or 10 seconds for any updates which the server has queued up. This switch is automatic during client login, but can take up to 45 seconds while the client waits for the server to call back and verify communication.

Individual clients

It is possible to force individual clients to start in polling mode, and hence avoid this delay. Edit the configuration file on the client and add the lines shown:

```
# Force client to poll.
smp.callback.passive
```

All clients

If you want to force all clients to start in polling mode, edit the configuration file on the server and add the lines shown:

```
# Force all clients to poll.
smp.callback.passive
```

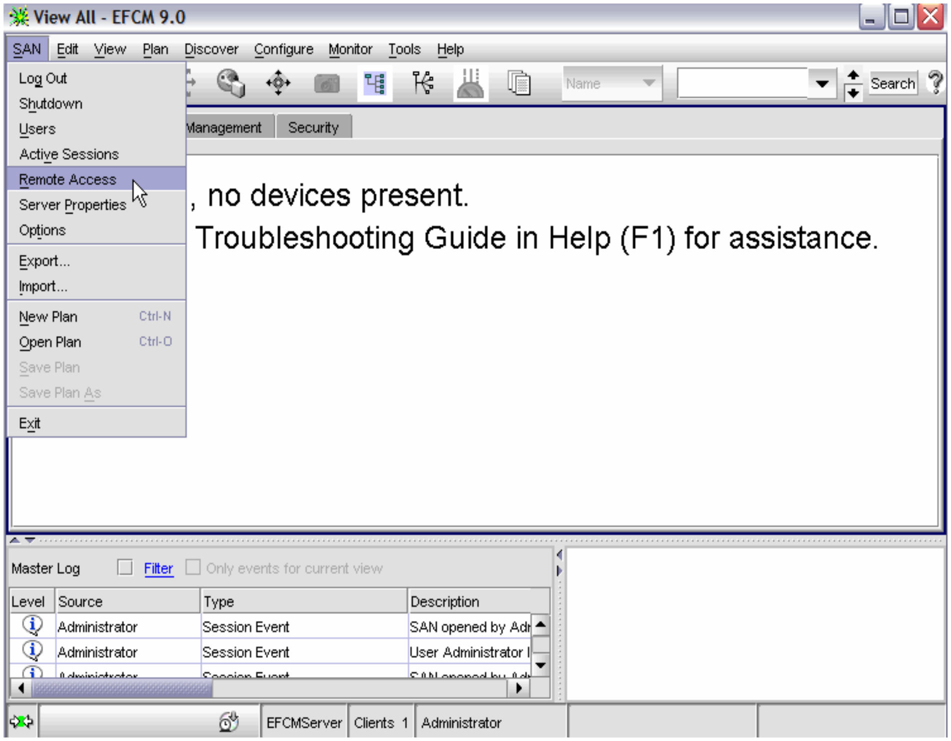
Remember to restart the EFCM Service.

> **Important:** Remember to re-apply these changes if you upgrade your EFCM software.

2.14.7 Defining EFCM user accounts

It is good practice with any application which supports user authentication that every user has their own account. This helps with the auditing of configuration changes, and also enables authority to be restricted to only that required for the job role. It also avoids the necessity of sharing passwords.

You can configure the number of remote client sessions allowed, up to a maximum of eight. You can also restrict remote session access by creating a list of allowed, or not allowed, TCP/IP addresses, or allowing access from any address. To do this select **SAN** → **Remote Access** and adjust the settings. Also make sure the *Allow remote management sessions box* is checked. See Figure 2-45.


View All - EFCM 9.0
SAN
Edit
View
Plan
Discover
Configure
Monitor
Tools
Help
Log Out
Shutdown
Users
Active Sessions
Remote Access
Server Properties
Options
Export...
Import...
New Plan Ctrl-N
Open Plan Ctrl-O
Save Plan
Save Plan As
Exit
Name
Search
Management
Security
Master Log
Filter
Only events for current view
EFCMServer
Clients 1
Administrator

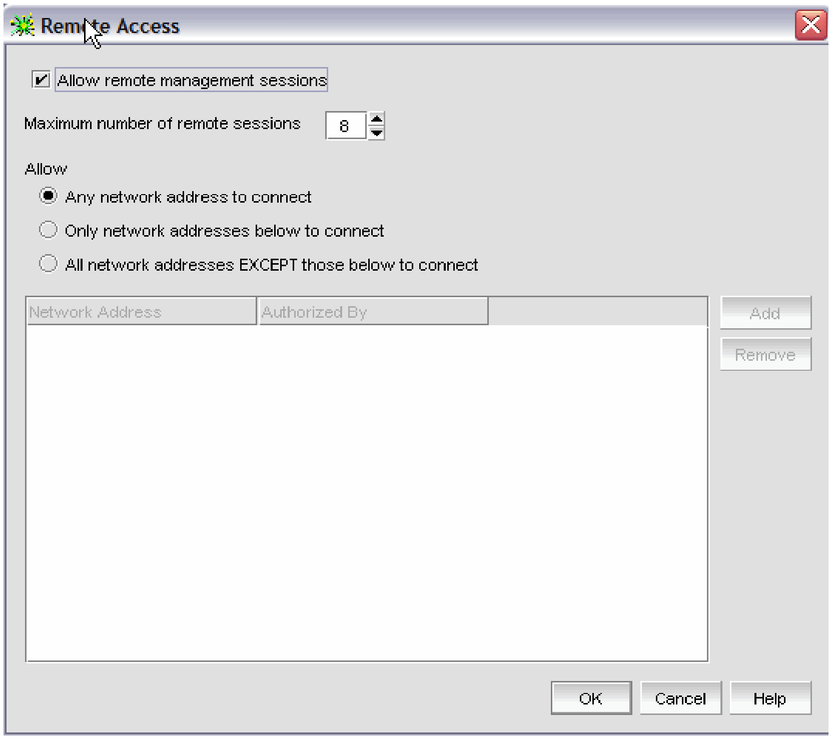
, no devices present.

Troubleshooting Guide in Help (F1) for assistance.

Level	Source	Type	Description
ⓘ	Administrator	Session Event	SAN opened by Adr
ⓘ	Administrator	Session Event	User Administrator l

Figure 2-45 Remote access

Also make sure the *Allow remote management sessions box* is checked as shown in Figure 2-46.



☑ Allow remote management sessions

Maximum number of remote sessions 8

Allow

● Any network address to connect

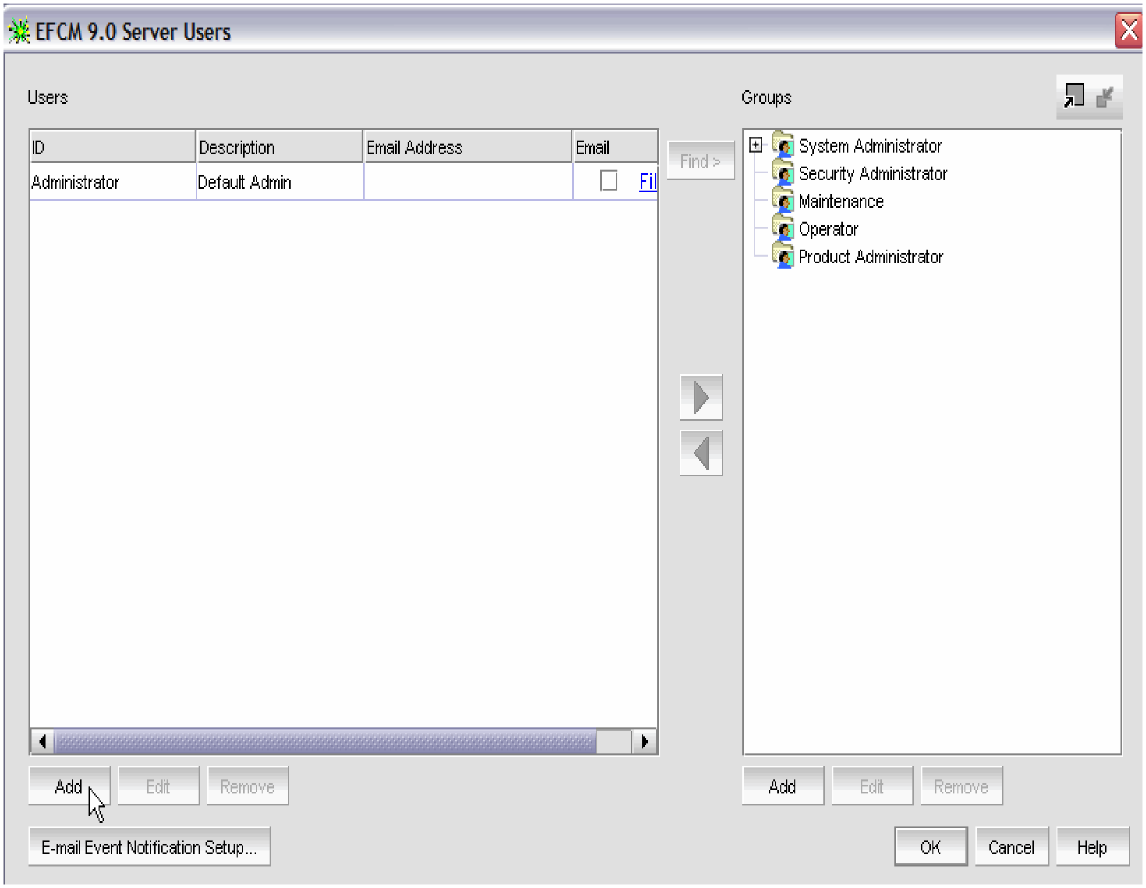
○ Only network addresses below to connect

○ All network addresses EXCEPT those below to connect

Network Address	Authorized By

Figure 2-46 Configuring remote access

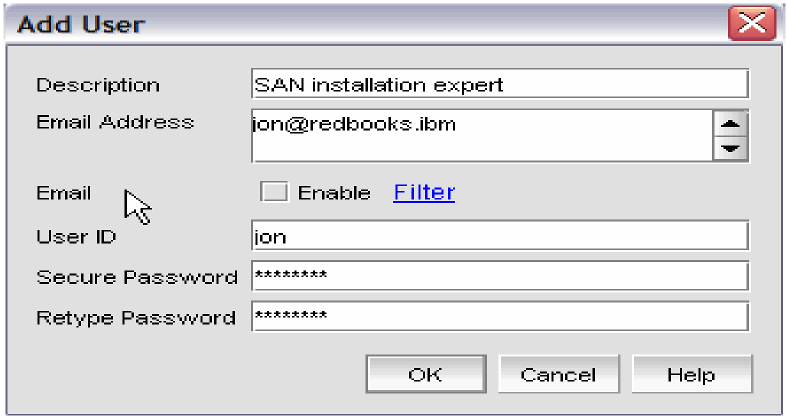
To modify the list of defined users, select **SAN** → **Users...** and you are presented with a list of defined users and the options to add users, modify existing users, view the rights of a user, and delete users. To add a new user, click the **Add** button as shown in Figure 2-47.


EFCM 9.0 Server Users
Users
Groups
Find >
System Administrator
Security Administrator
Maintenance
Operator
Product Administrator
Add
Edit
Remove
Add
Edit
Remove
E-mail Event Notification Setup...
OK
Cancel
Help

ID	Description	Email Address	Email
Administrator	Default Admin		☐ Fil

Figure 2-47 Adding a new user

Figure 2-48 shows the addition of a new user called *jon*.

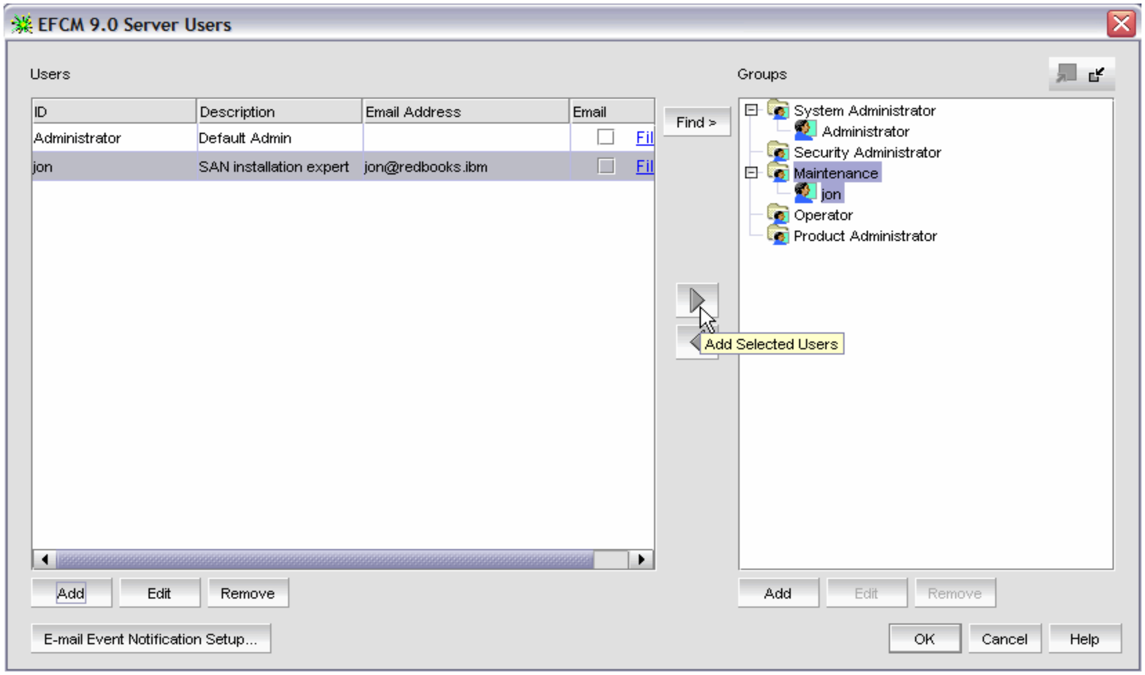

Add User

Description: SAN installation expert
Email Address: jon@redbooks.ibm
Email: ☐ Enable Filter
User ID: jon
Secure Password: ********
Retype Password: ********

OK
Cancel
Help

Figure 2-48 Adding a new user

To assign authority to this user, highlight the ID in the left-hand panel, and the desired group in the right-hand panel, and click the arrow to add the user to the group as shown in Figure 2-49. Finally, click **OK** to commit the change.


EFCM 9.0 Server Users
Users
Groups

ID	Description	Email Address	Email	
Administrator	Default Admin		☐	Fil
jon	SAN installation expert	jon@redbooks.ibm	☐	Fil

System Administrator
Administrator
Security Administrator
Maintenance
jon
Operator
Product Administrator
Find >
Add Selected Users
Add
Edit
Remove
E-mail Event Notification Setup...
Add
Edit
Remove
OK
Cancel
Help

Figure 2-49 Addition of new user to a user group

2.14.8 Assigning user rights

The pre-defined user rights are:

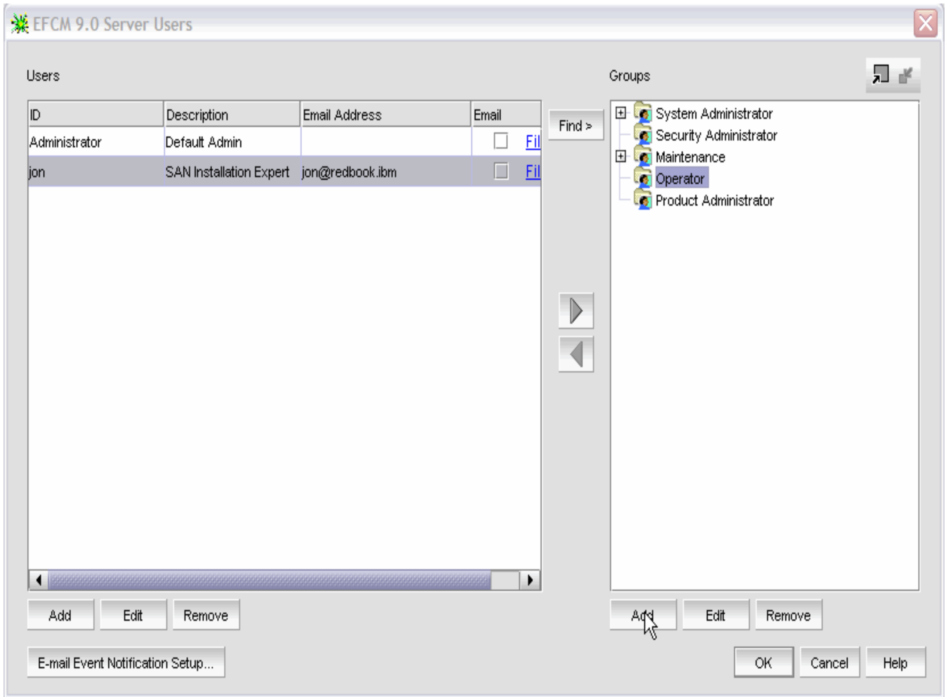
- System Administrator
- Security Administrator
- Maintenance
- Operator
- Product Administrator

The *System Administrator* right grants access to every control and configuration task that has to be performed from within the EFC Manager and can be viewed as the highest level of authority. It only has “view” rights while operating in an Element Manager application. Here we require the *Product Administrator* right to perform changes.

All new users initially have view rights and this cannot be removed. For a table of user rights of Element Manager functions, refer to the *McDATA EFC Manager Software User Manual*, P/N 620-000170.

In addition to the pre-defined user rights as above, an administrator can make up their own user name and configure any rights to this user.

To add a new user group, select the **Add** option at the bottom of the group section as shown in Figure 2-50.

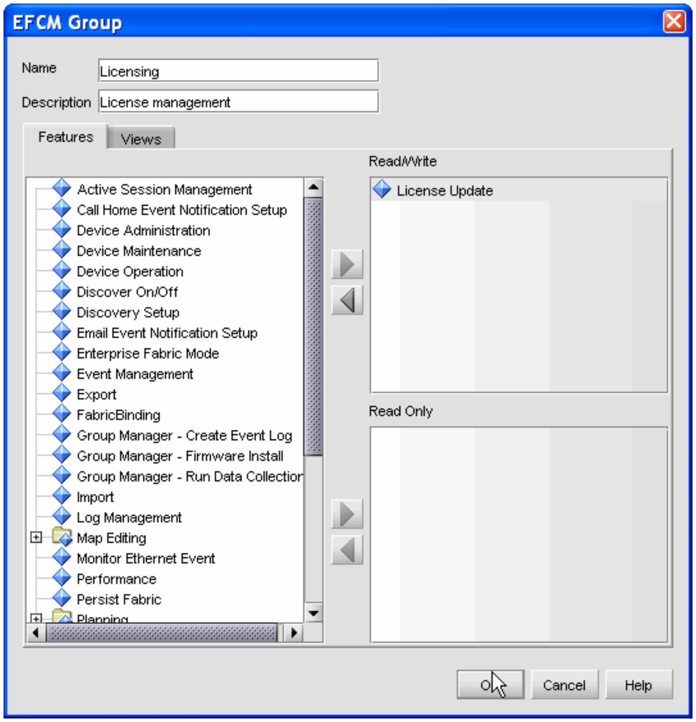

EFCM 9.0 Server Users
Users
Groups
Find >
Add
Edit
Remove
E-mail Event Notification Setup...
Add
Edit
Remove
OK
Cancel
Help

ID	Description	Email Address	Email
Administrator	Default Admin		☐ Fil
jon	SAN Installation Expert	jon@redbook.ibm	☐ Fil

- System Administrator
- Security Administrator
- Maintenance
- Operator
- Product Administrator

Figure 2-50 Adding a new group selection

From the window that is displayed, you can create new groups, as well as select which features this group has access to. You can also select whether this group can have read only access or read write access. An example is shown in Figure 2-51.



Name: Licensing

Description: License management

- Active Session Management
- Call Home Event Notification Setup
- Device Administration
- Device Maintenance
- Device Operation
- Discover On/Off
- Discovery Setup
- Email Event Notification Setup
- Enterprise Fabric Mode
- Event Management
- Export
- FabricBinding
- Group Manager - Create Event Log
- Group Manager - Firmware Install
- Group Manager - Run Data Collection
- Import
- Log Management
- Map Editing
- Monitor Ethernet Event
- Performance
- Persist Fabric
- Planning

Read/Write: License Update

Figure 2-51 Adding a new group

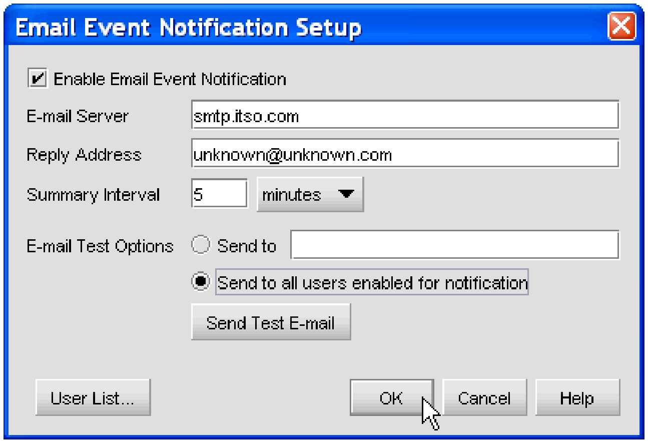
2.14.9 EFCM event notification

In this section we discuss the EFCM event notification options.

E-mail notification

The EFCM server can be configured to generate e-mail alerts for various events. To do this select **Monitor** → **Event Notification** → **Email**.

Check the **Enable Email Event Notification** check box, as shown in Figure 2-52, and change the *Summary Interval* to an acceptable value.



☑ Enable Email Event Notification
E-mail Server: smtp.itso.com
Reply Address: unknown@unknown.com
Summary Interval: 5 minutes
E-mail Test Options: ○ Send to
● Send to all users enabled for notification

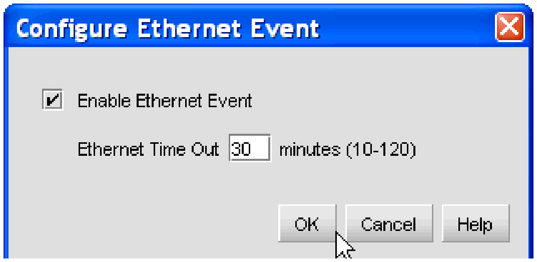
Figure 2-52 EFCM Email Event Notification

Now click the **User List...** button to open the Server Users window. For each user that should receive the event e-mail, check the **Email** check box. Optionally, also click the **Filter** link to modify the event classes to be alerted for. Ensure that the user has an *Email Address* defined, and click **OK** to return to the setup window.

Select the **Send to all users enabled for notification** radio button and then click the **Send Test E-mail** button. Each configured user should now receive a test e-mail. Finally, click **OK** to close the window.

Ethernet events

By selecting **Monitor** → **Ethernet Event** and checking the **Enable Ethernet Event** check box, you can configure the EFCM server to alert if it loses Ethernet connection to a managed device for longer than the specified time-out interval, as shown in Figure 2-53.



☑ Enable Ethernet Event
Ethernet Time Out 30 minutes (10-120)

Figure 2-53 Enabling Ethernet events

2.14.10 Initial switch network configuration

Now that the EFCM server has been installed, we can start installation of the first fabric device.

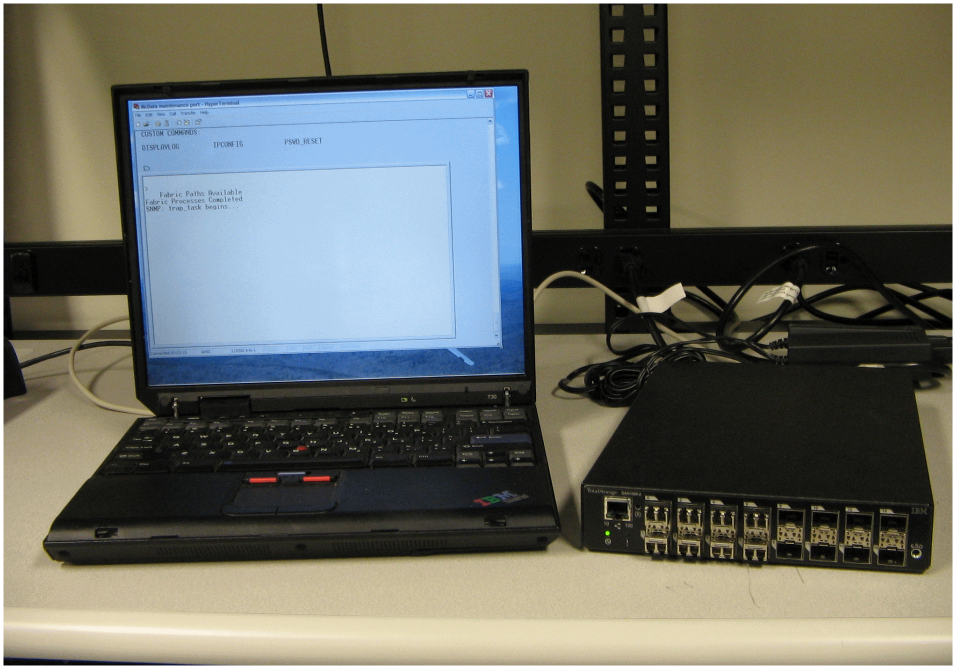
> **Tip:** Even if this is currently your only switch, we strongly recommend that you attach an identifying label to the front of the switch. This name can be used later when defining the switch to the EFC Manager.

As previously mentioned, the switch is delivered with a default TCP/IP configuration that normally requires changing to suit the installation environment. There are two ways to achieve this, either via the maintenance port and a null-modem cable, or with the new SANplicity Wizard and a network cross-over cable.

Maintenance port

This connects the RS-232 maintenance port and a suitable workstation using a null-modem cable, and a terminal emulator. In this example we use the Windows HyperTerminal application.

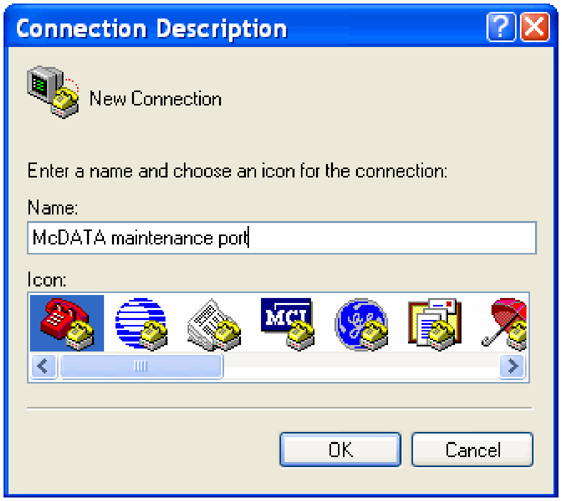
Figure 2-54 shows the equipment used for the following procedure.


McData maintenance port - HyperTerminal
File Edit View Call Transfer Help

```
CUSTOM COMMANDS:

DISPLAYLOG          IPCONFIG          PSWD_RESET

C>

>
    Fabric Paths Available
Fabric Processes Completed
SNMP: trap_task begins...
```

Figure 2-54 HyperTerminal connected to SAN16M-2

Connect the workstation to the maintenance port using the supplied null modem cable and launch HyperTerminal. Enter a suitable name, as shown in Figure 2-55 and click **OK**.

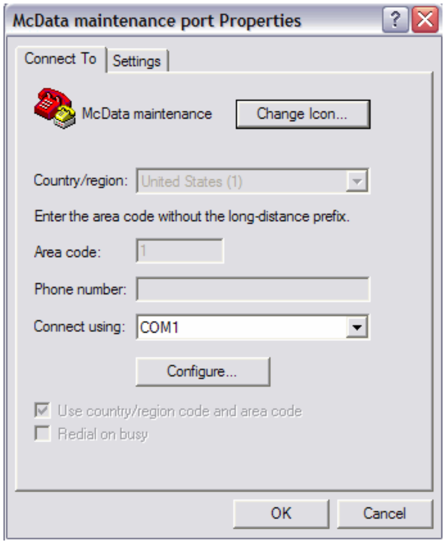

Connection Description
New Connection
Icon:
OK
Cancel

Enter a name and choose an icon for the connection:

Name: McDATA maintenance port

Figure 2-55 HyperTerminal start up

Change the port selection to the appropriate COM*X* port, as shown in Figure 2-56, and click **OK**.


McData maintenance port Properties
Connect To
Settings
McData maintenance
Change Icon...
Configure...
OK
Cancel

Country/region: United States (1)

Enter the area code without the long-distance prefix.

Area code: 1

Phone number:

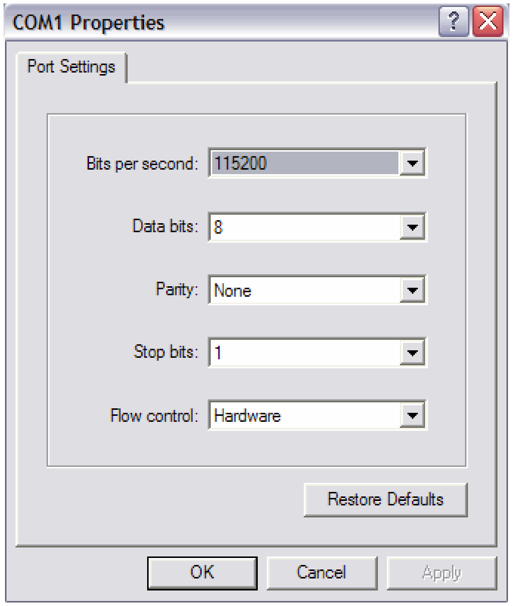
Connect using: COM1

☑ Use country/region code and area code

☐ Redial on busy

Figure 2-56 HyperTerminal port selection

Set the port characteristics as shown in Figure 2-57 and click **OK** to start the session.


COM1 Properties
Port Settings
Restore Defaults
OK
Cancel
Apply

Bits per second: 115200

Data bits: 8

Parity: None

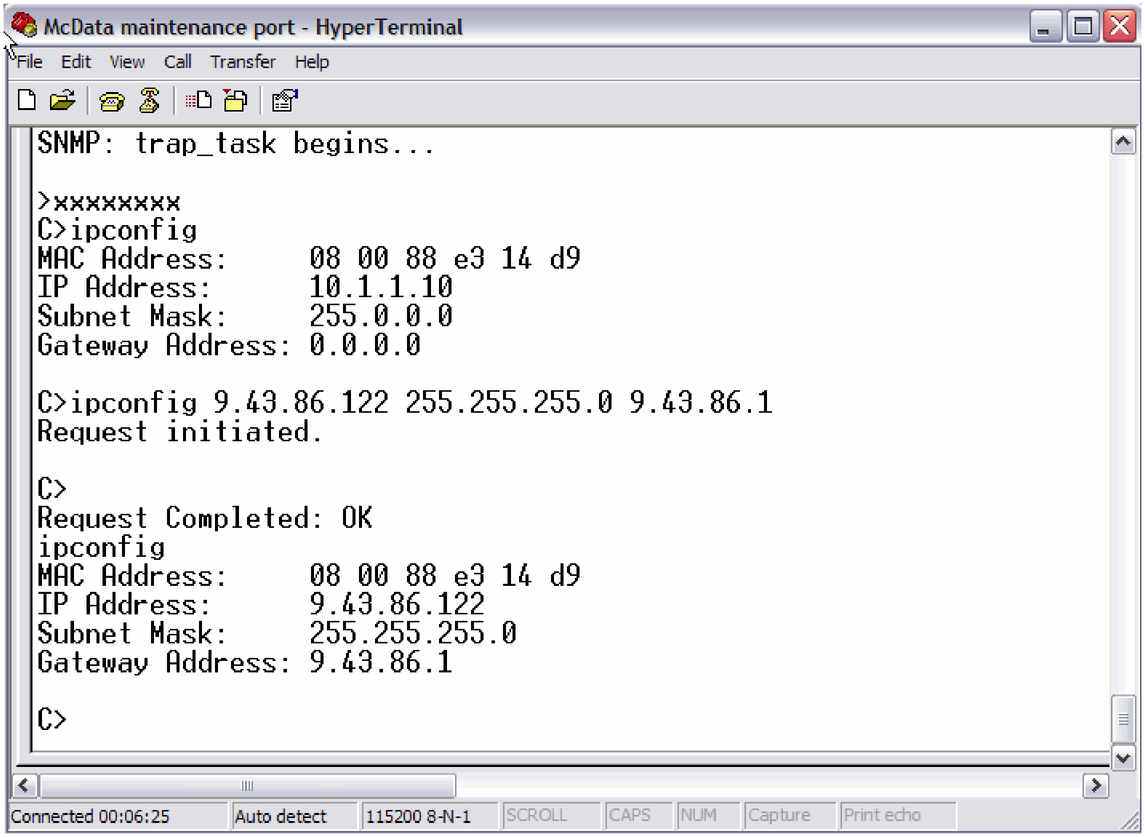
Stop bits: 1

Flow control: Hardware

Figure 2-57 HyperTerminal port properties

Note: Older hardware might require a data rate of 57600 instead of 115200.

Figure 2-58 shows an example dialogue for the setup procedure.


McData maintenance port - HyperTerminal
File Edit View Call Transfer Help
Connected 00:06:25
Auto detect
115200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
SNMP: trap_task begins...

>xxxxxxxx
C>ipconfig
MAC Address:     08 00 88 e3 14 d9
IP Address:      10.1.1.10
Subnet Mask:     255.0.0.0
Gateway Address: 0.0.0.0

C>ipconfig 9.43.86.122 255.255.255.0 9.43.86.1
Request initiated.

C>
Request Completed: OK
ipconfig
MAC Address:     08 00 88 e3 14 d9
IP Address:      9.43.86.122
Subnet Mask:     255.255.255.0
Gateway Address: 9.43.86.1

C>
```

Figure 2-58 HyperTerminal session changing default TCP/IP settings

Usernames are not required for the maintenance port; the level of access gained is by recognizing the password used. At the **>** prompt, type the user-level password (the default is `password` and is case-sensitive) and press Enter; a **C>** prompt should appear. Run the **`ipconfig`** command to display the current IP settings. If the settings require changing, re-enter the **`ipconfig`** command with the appropriate values, in the format:

```
ipconfig address subnet_mask gateway
```

If you want, you can run the **`ipconfig`** command again to confirm the change. Enter the **`exit`** command and close the session.

> **Tip:** You might want to save the HyperTerminal session definition if you intend to configure more switches.

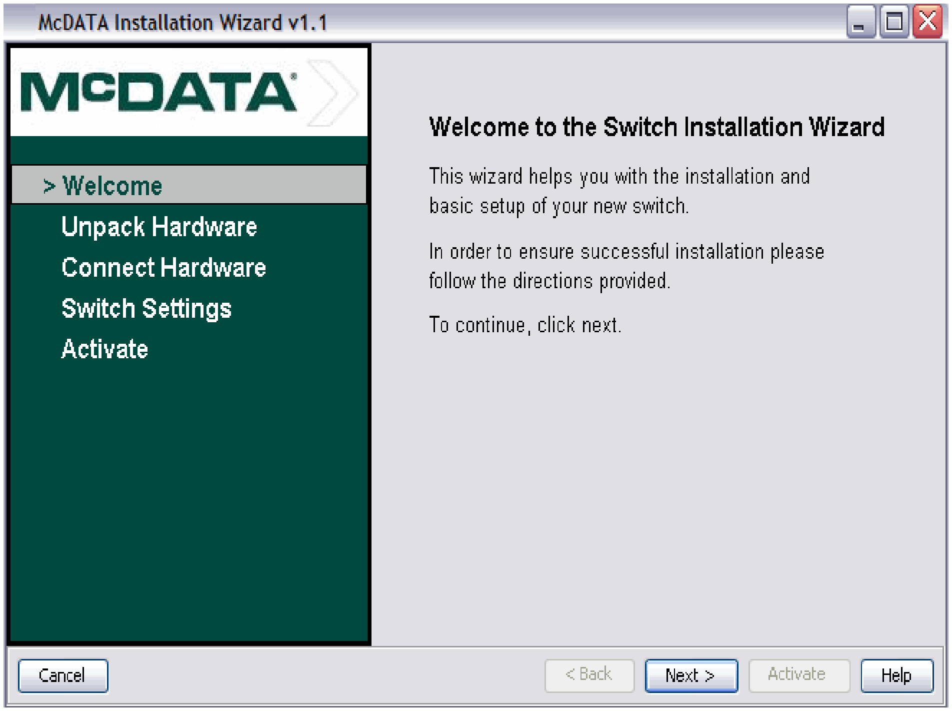
You can now remove the null modem cable and connect the switch's Ethernet cable to the network. Replace the dust cap on the switch's RS-232 (if if had one.) Then you can proceed with switch configuration using either EFCM Basic or the EFCM server.

Tip: Full details of this process are provided in the "Installation Tasks" chapter of the relevant *McDATA Installation and Service Manual*.

SANplicity Wizard

As an alternative to using the maintenance port for initial network configuration, the new SANplicity Wizard allows initial switch configuration to be carried out with a direct network connection using the supplied cross-over cable. The wizard is a small Java application that requires Java Runtime Environment (JRE™) version 1.3 or later, and is qualified for Windows and Solaris. This wizard is on the software CD supplied with the switch, or you can obtain it from the McDATA website (see "Obtaining software, firmware, and documentation" on page 472 for details of the Web site).

If necessary, unzip the file and launch the wizard from the `SANplicityWizard.jar` file. You should see the welcome window shown in Figure 2-59.



Welcome to the Switch Installation Wizard

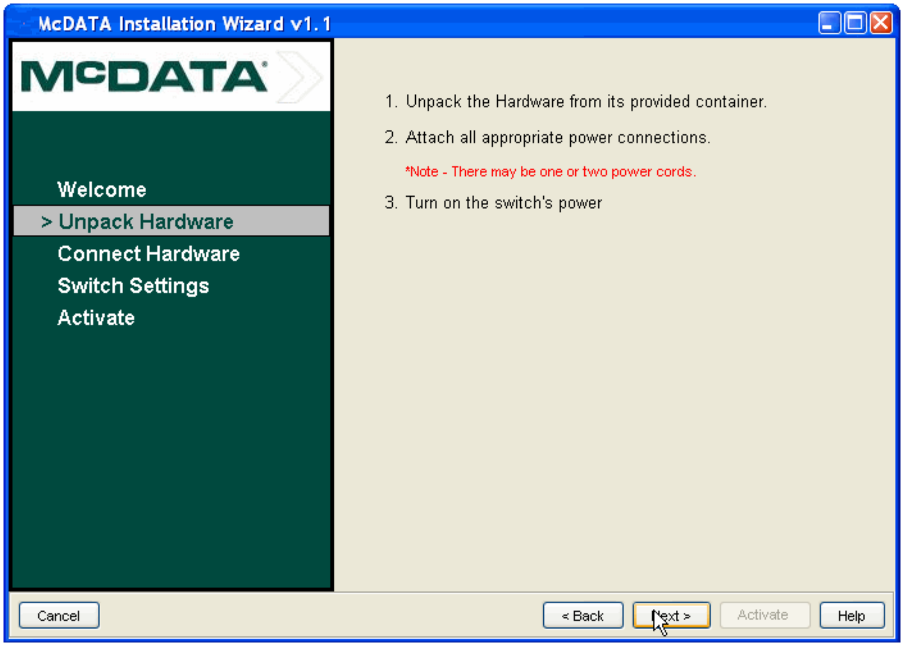
This wizard helps you with the installation and basic setup of your new switch.

In order to ensure successful installation please follow the directions provided.

To continue, click next.

Figure 2-59 SANplicity Wizard welcome window

After reading the welcome window, click **Next >** to proceed to the step shown in Figure 2-60. Make sure all the hardware is unpacked and powered up then, click **Next** to proceed to test the connection.


McDATA Installation Wizard v1.1
McDATA
Welcome
> Unpack Hardware
Connect Hardware
Switch Settings
Activate
Cancel
< Back
Next >
Activate
Help

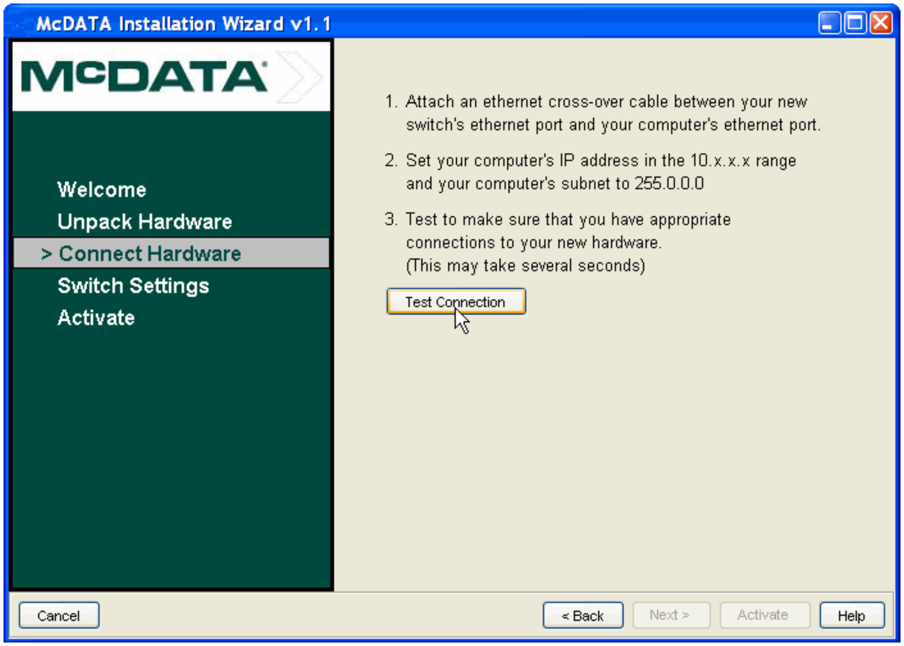
1. Unpack the Hardware from its provided container.
2. Attach all appropriate power connections.

*Note - There may be one or two power cords.

3. Turn on the switch's power

Figure 2-60 SANplicity Wizard unpack window

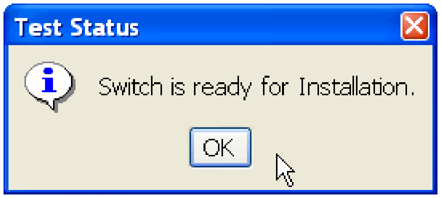
Plug in the cross-over cable as instructed and click the **Test Connection** button, as shown in Figure 2-61.


McDATA Installation Wizard v1.1
MCDATA
Welcome
Unpack Hardware
> Connect Hardware
Switch Settings
Activate
Test Connection
Cancel
< Back
Next >
Activate
Help

1. Attach an ethernet cross-over cable between your new switch's ethernet port and your computer's ethernet port.
2. Set your computer's IP address in the 10.x.x.x range and your computer's subnet to 255.0.0.0
3. Test to make sure that you have appropriate connections to your new hardware. (This may take several seconds)

Figure 2-61 SANplicity Wizard connection window

When the test is successful, you should see the status in Figure 2-62. Click **OK**.


Test Status
OK

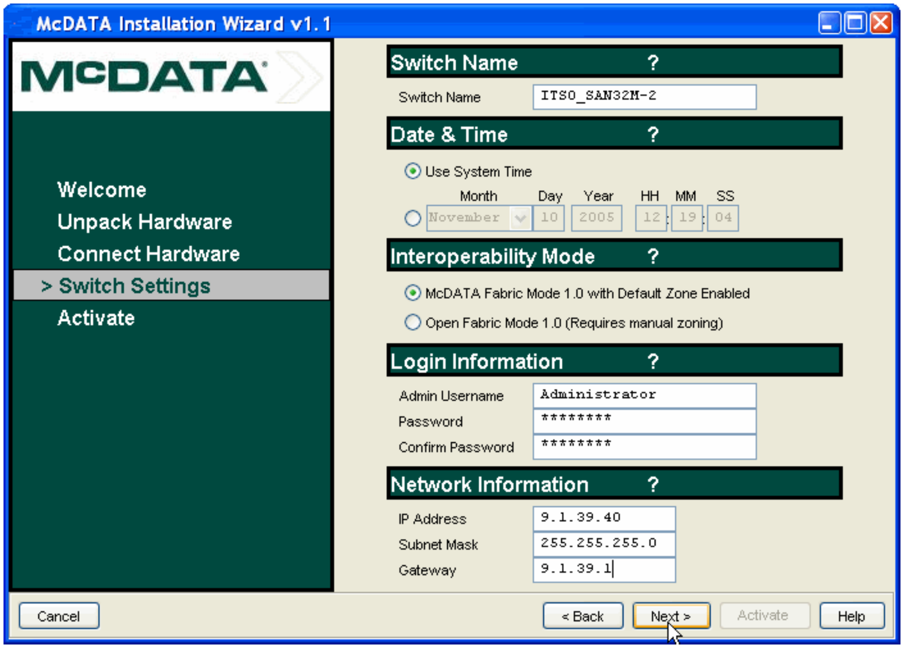
Switch is ready for Installation.

Figure 2-62 Connection tested

Now click **Next**, from the window shown in Figure 2-61, to proceed to the next step.

> **Note:** If you have a software firewall installed, you might have to authorize the `javaw.exe` process.

Complete all the fields with the correct values in the window shown in Figure 2-63, review it, and click **Next >** to proceed to **Activation**.


McDATA Installation Wizard v1.1
MCDATA
Welcome
Unpack Hardware
Connect Hardware
> Switch Settings
Activate
Switch Name ?
Date & Time ?
Interoperability Mode ?
Login Information ?
Network Information ?
Cancel
< Back
Next >
Activate
Help

Switch Name: ITSO_SAN32M-2

● Use System Time

○ Month: November Day: 10 Year: 2005 HH: 12 MM: 19 SS: 04

● McDATA Fabric Mode 1.0 with Default Zone Enabled

○ Open Fabric Mode 1.0 (Requires manual zoning)

Admin Username: Administrator

Password: ********

Confirm Password: ********

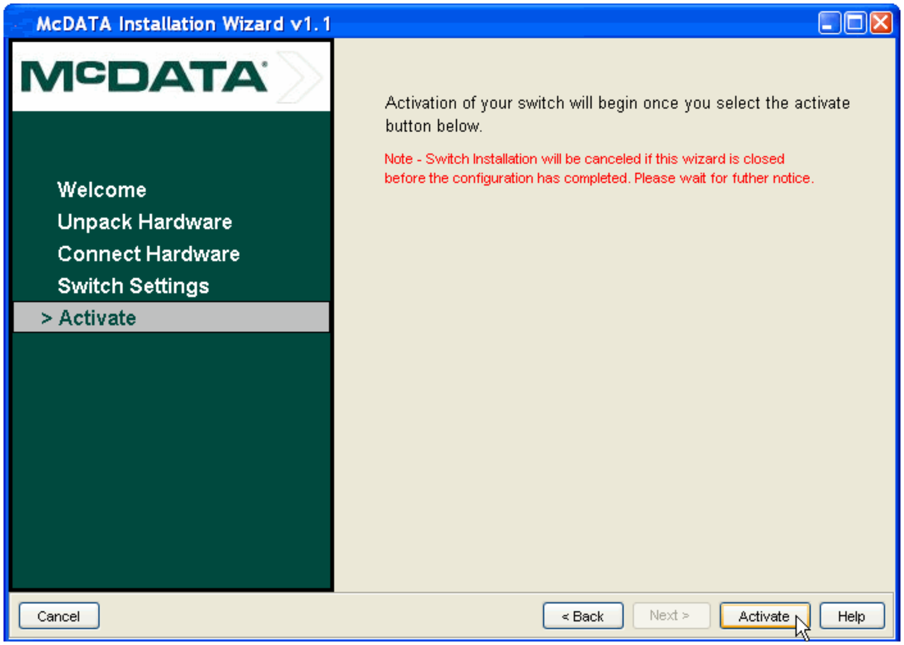
IP Address: 9.1.39.40

Subnet Mask: 255.255.255.0

Gateway: 9.1.39.1

Figure 2-63 SANplicity Wizard switch settings window

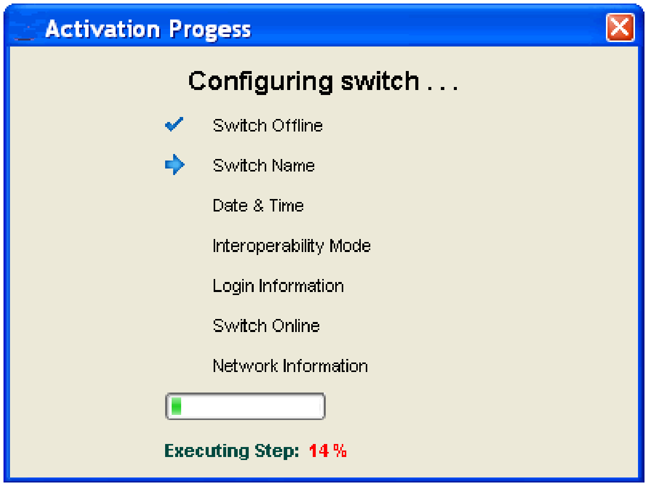
Click **Activate** as shown in Figure 2-64, and the progress window shown in Figure 2-65 displays.


McDATA Installation Wizard v1.1
MCDATA
Welcome
Unpack Hardware
Connect Hardware
Switch Settings
> Activate
Cancel
< Back
Next >
Activate
Help

Activation of your switch will begin once you select the activate button below.

Note - Switch Installation will be canceled if this wizard is closed before the configuration has completed. Please wait for futher notice.

Figure 2-64 SANplicity Wizard activation window


Activation Progess

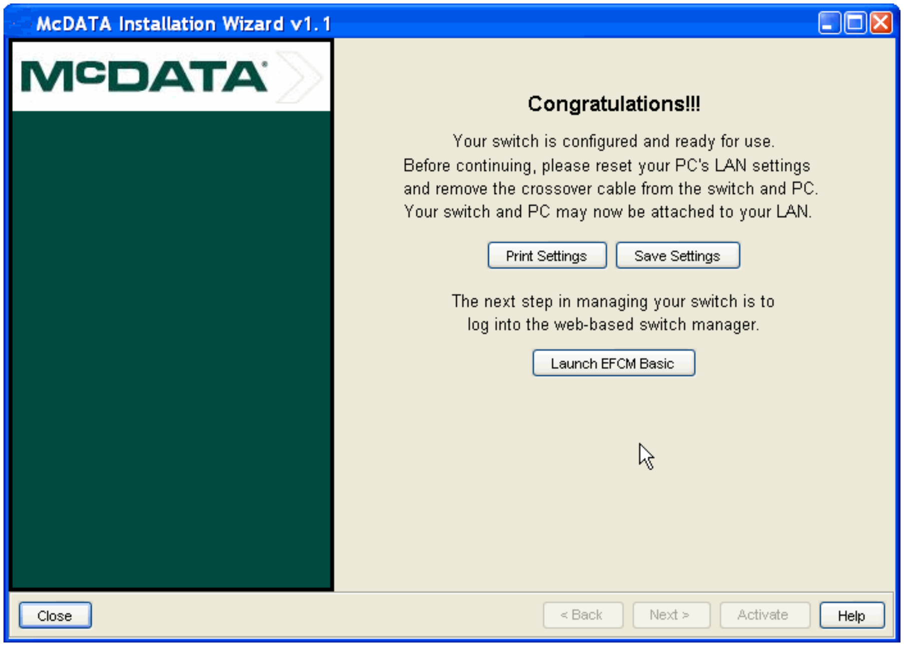
Configuring switch . . .

- ✓ Switch Offline
- ➡ Switch Name
- Date & Time
- Interoperability Mode
- Login Information
- Switch Online
- Network Information

Executing Step: 14 %

Figure 2-65 SANplicity Wizard activation progress

Finally, the window shown in Figure 2-66 displays. You should now remove the cross-over cable and connect the switch to your network using a normal cable.


McDATA Installation Wizard v1.1
MCDATA

Congratulations!!!

Your switch is configured and ready for use.
Before continuing, please reset your PC's LAN settings
and remove the crossover cable from the switch and PC.
Your switch and PC may now be attached to your LAN.

Print Settings
Save Settings

The next step in managing your switch is to
log into the web-based switch manager.

Launch EFCM Basic
Close
< Back
Next >
Activate
Help

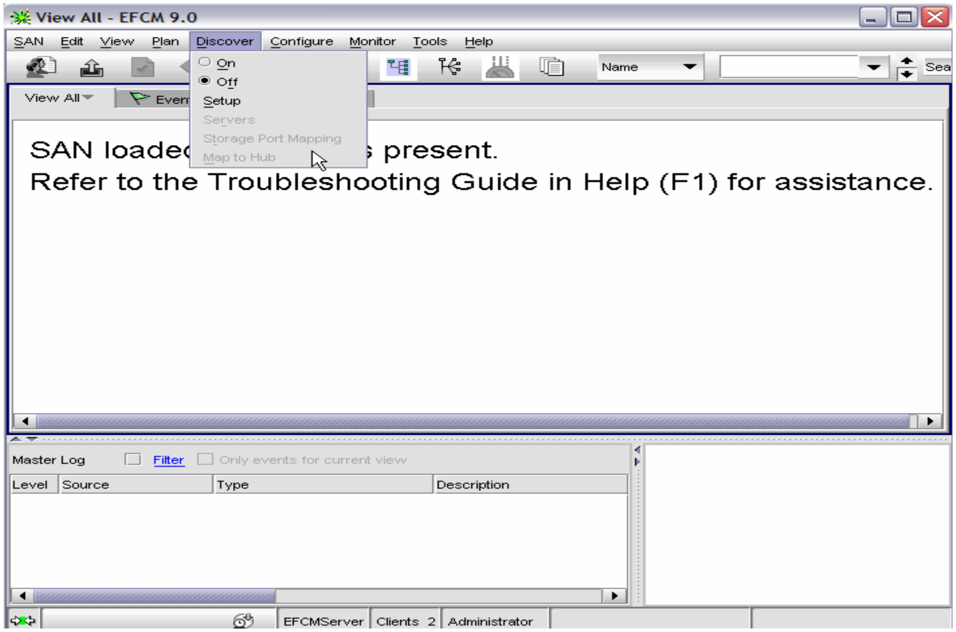
Figure 2-66 SANplicity Wizard completion

You can now proceed with switch configuration using either EFCM Basic or the EFCM server.

2.14.11 Discovering the switch with EFC Manager

Now that the switch or director is on the network, it can be discovered by the EFCM server.

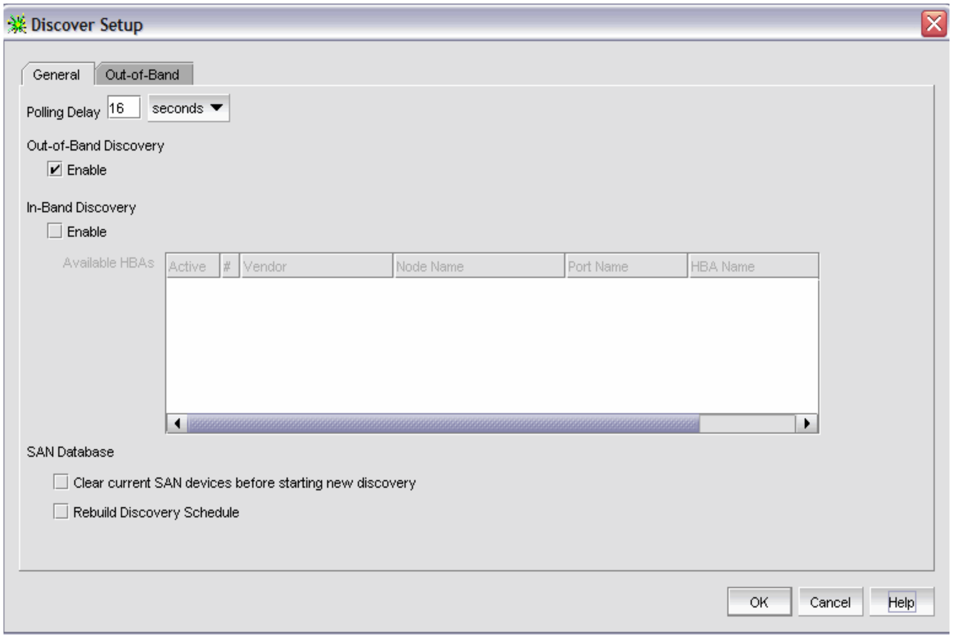
Launch the EFCM client and logon to the server. As this is our first switch, the SAN view is empty. Click **Discover** → **Setup...** as shown in Figure 2-67.


View All - EFCM 9.0
SAN
Edit
View
Plan
Discover
Configure
Monitor
Tools
Help
○ On
● Off
Setup
Servers
Storage Port Mapping
Map to Hub
Name
Sea
View All
Even
Master Log
☐ Filter
☐ Only events for current view
Level
Source
Type
Description
EFCMServer
Clients 2
Administrator

SAN loade s present.
Refer to the Troubleshooting Guide in Help (F1) for assistance.

Figure 2-67 EFC Manager, Discover Setup...

This takes you to the Discover Setup window, shown in Figure 2-68. Ensure that the Out-of-Band Discovery option is selected; if not, select the Out-of-Band tab. Click **OK** to continue.


Discover Setup
General
Out-of-Band

Polling Delay 16 seconds

Out-of-Band Discovery

☑ Enable

In-Band Discovery

☐ Enable

Available HBAs
Active
#
Vendor
Node Name
Port Name
HBA Name

SAN Database

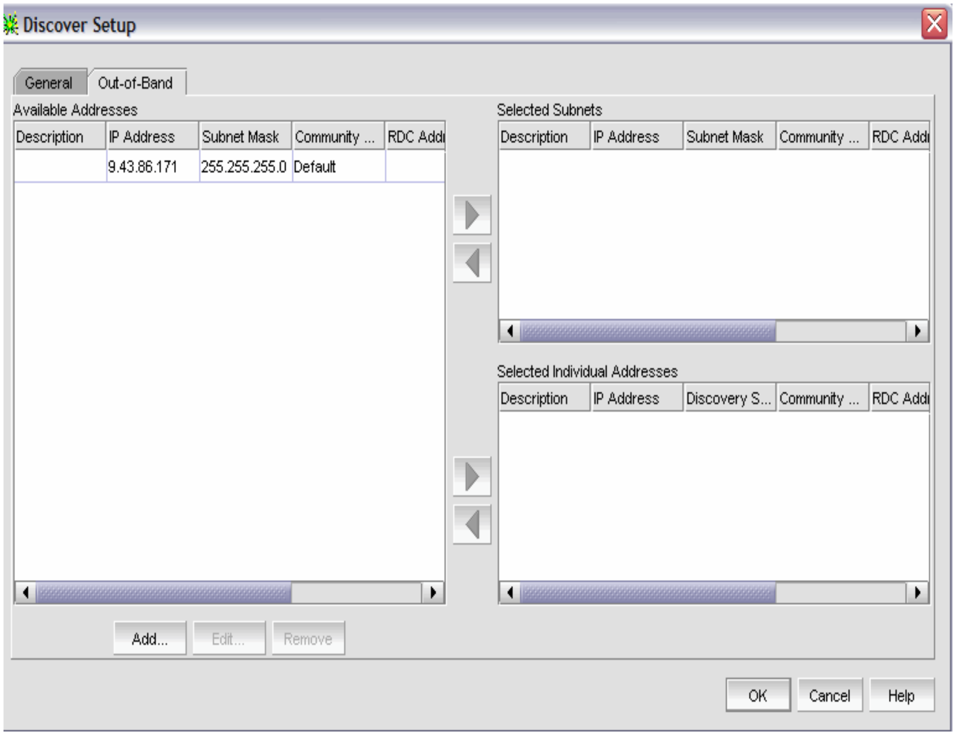
☐ Clear current SAN devices before starting new discovery

☐ Rebuild Discovery Schedule

OK
Cancel
Help

Figure 2-68 Discover Setup window

Selecting this takes us to the Discover Out-of-Band Setup window, where we click the **Add** button... as shown in Figure 2-69.



Discover Setup
General
Out-of-Band
Available Addresses
Selected Subnets
Selected Individual Addresses
Add...
Edit...
Remove
OK
Cancel
Help

Available Addresses

Description	IP Address	Subnet Mask	Community ...	RDC Addr
	9.43.86.171	255.255.255.0	Default	

Selected Subnets

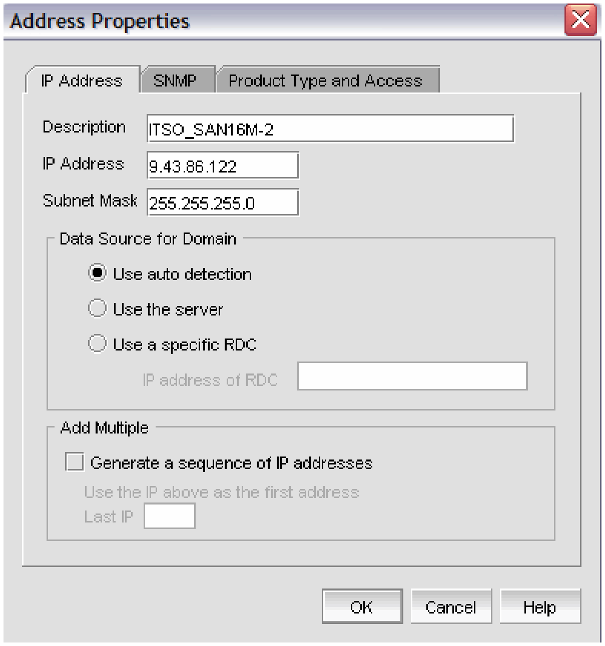
Description	IP Address	Subnet Mask	Community ...	RDC Addr

Selected Individual Addresses

Description	IP Address	Discovery S...	Community ...	RDC Addr

Figure 2-69 Discover Out-of-Band Setup

This brings up the Address Properties input box for the new device, as shown in Figure 2-70. Here we fill in a name and the IP address of the switch that we want to add. At this stage leave the **SNMP** and **Product Type and Access** tabs with their default values.



Description: ITSO_SAN16M-2

IP Address: 9.43.86.122

Subnet Mask: 255.255.255.0

Data Source for Domain

● Use auto detection

○ Use the server

○ Use a specific RDC

IP address of RDC

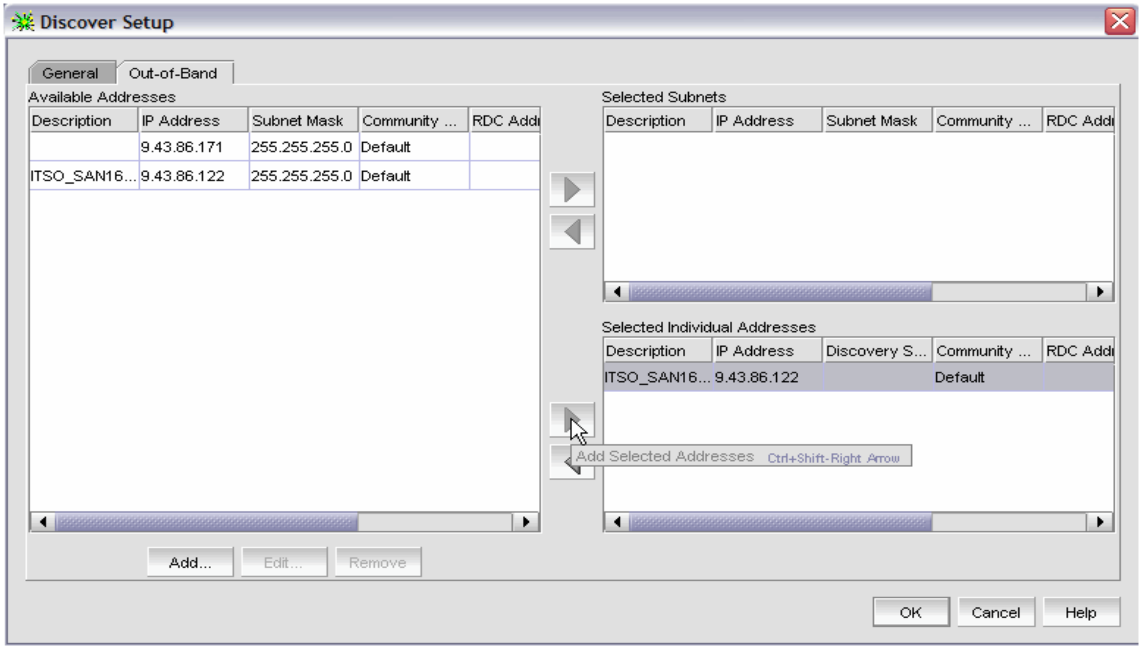
Add Multiple

☐ Generate a sequence of IP addresses

Address Properties
IP Address
SNMP
Product Type and Access
Use the IP above as the first address
Last IP
OK
Cancel
Help

Figure 2-70 Defining new SAN24M-2 with its IP address

The device then shows in the Available Addresses window on the left. Next we click the device we want to manage and then click the arrow to add the device to the Selected Individual Addresses window on the right and click **OK**. This is shown in Figure 2-71.


Discover Setup
General
Out-of-Band
Add Selected Addresses Ctrl+Shift-Right Arrow
Add...
Edit...
Remove
OK
Cancel
Help

Available Addresses

Description	IP Address	Subnet Mask	Community ...	RDC Add
	9.43.86.171	255.255.255.0	Default	
ITSO_SAN16...	9.43.86.122	255.255.255.0	Default	

Selected Subnets

Description	IP Address	Subnet Mask	Community ...	RDC Add

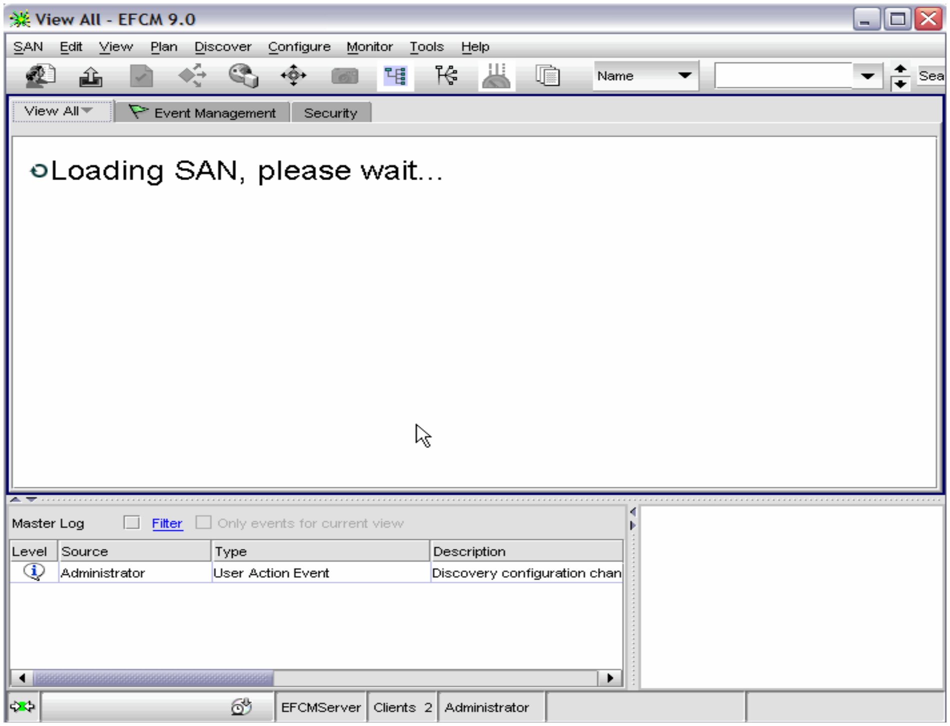
Selected Individual Addresses

Description	IP Address	Discovery S...	Community ...	RDC Add
ITSO_SAN16...	9.43.86.122		Default	

Figure 2-71 Adding device to Selected Individual Addresses

You also have the option in the window to add a complete IP subnet; this is so you can auto discover all switches in this IP subnet without having to individually add each one manually. To do this, select the switch you have added into the **Selected Subnet** field.

The EFCM now reloads the SAN, as shown in Figure 2-72, which takes a few seconds.


View All - EFCM 9.0
SAN Edit View Plan Discover Configure Monitor Tools Help
Name
Sea
View All
Event Management
Security

Loading SAN, please wait...

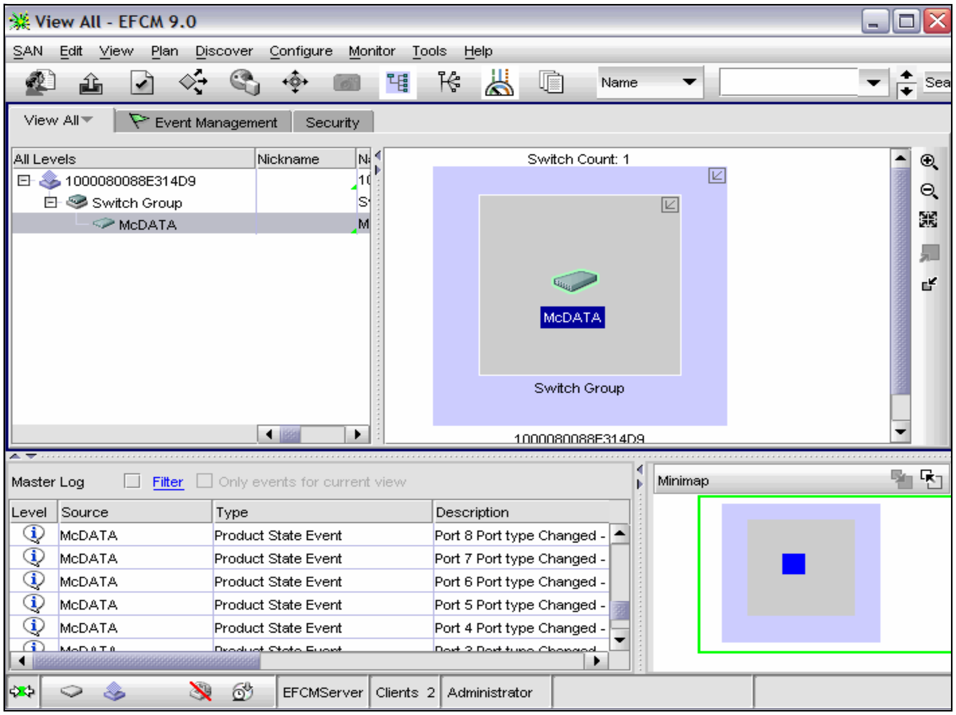
Master Log
Filter
Only events for current view

Level	Source	Type	Description
ⓘ	Administrator	User Action Event	Discovery configuration chan

EFCMServer
Clients 2
Administrator

Figure 2-72 SAN reloading after discovery setup

The new device now displays as shown in Figure 2-73.


View All - EFCM 9.0
SAN
Edit
View
Plan
Discover
Configure
Monitor
Tools
Help
Name
Sea
View All
Event Management
Security
All Levels
Nickname
1000080088E314D9
Switch Group
McDATA
Switch Count: 1
McDATA
Switch Group
1000080088E314D9
Master Log
Filter
Only events for current view
Minimap
EFCMServer
Clients 2
Administrator

Level	Source	Type	Description
ⓘ	McDATA	Product State Event	Port 8 Port type Changed -
ⓘ	McDATA	Product State Event	Port 7 Port type Changed -
ⓘ	McDATA	Product State Event	Port 6 Port type Changed -
ⓘ	McDATA	Product State Event	Port 5 Port type Changed -
ⓘ	McDATA	Product State Event	Port 4 Port type Changed -
ⓘ	McDATA	Product State Event	Port 3 Port type Changed

Figure 2-73 SAN loaded

You are now ready to continue configuration of the switch.

2.14.12 Feature installation and licensing

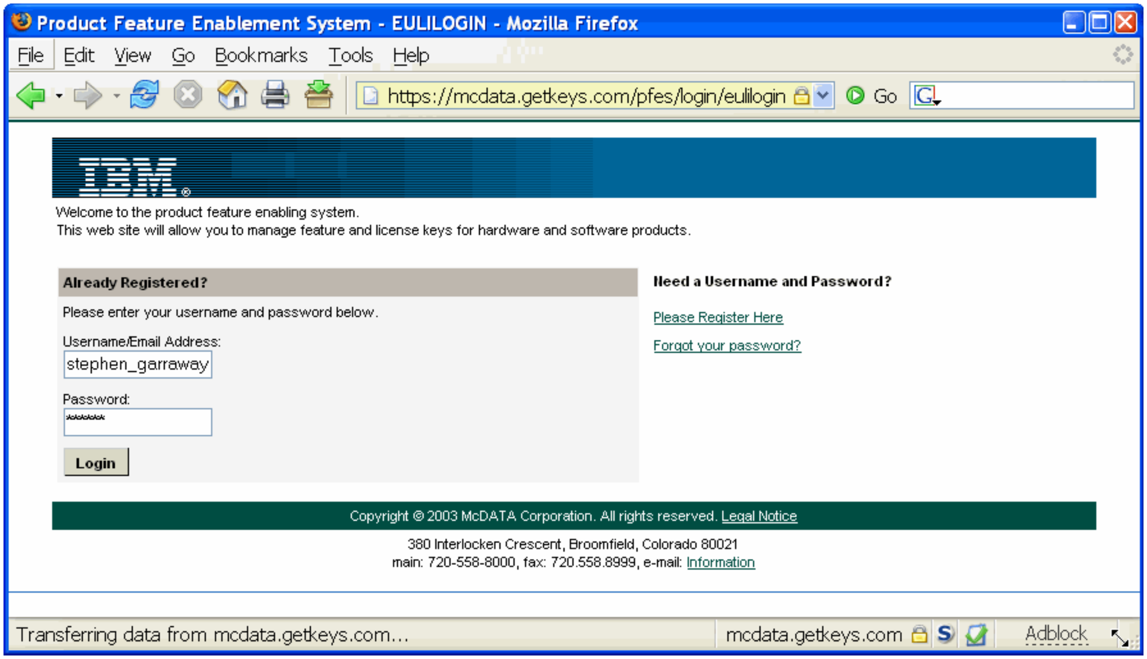
IBM m-type switches support several optional features that are licensable by purchasing transaction codes (in the format xxx-xxx-xxx), which are used to generate a product feature enablement (PFE) key. These codes are purchased for a given switch or director model, and then used to generate a key specific to the serial number of the switch.

The transaction codes are delivered as a piece of paper showing the hardware model and the code. If several features are purchased at the same time for the same product, a matching number of transaction codes are assigned.

Key generation

If a feature key is not supplied, then it can be generated using the transaction codes and the model and serial number of the switch or director. This is done using a form on the McDATA Product Feature Enablement Web site shown in Figure 2-74. You are required to register with this site to gain access; this is a free service.

`http://mcdata.getkeys.com/ibm`



Product Feature Enablement System - EULILOGIN - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Go
IBM

https://mcdata.getkeys.com/pfes/login/eulilogin

Welcome to the product feature enabling system.
This web site will allow you to manage feature and license keys for hardware and software products.

Already Registered?

Please enter your username and password below.

Username/Email Address: stephen_garraway

Password: ******

Login

Need a Username and Password?

Please Register Here
Forgot your password?

Copyright © 2003 McDATA Corporation. All rights reserved. Legal Notice

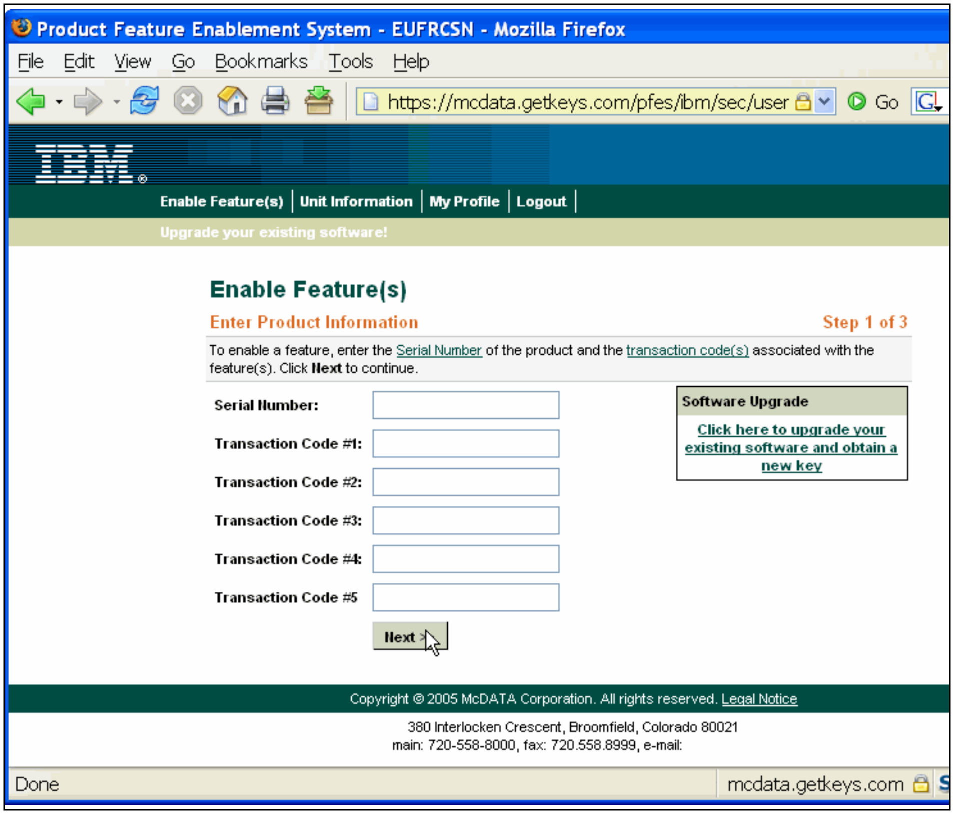
380 Interlocken Crescent, Broomfield, Colorado 80021
main: 720-558-8000, fax: 720.558.8999, e-mail: Information

Transferring data from mcdata.getkeys.com...

mcdata.getkeys.com
Adblock

Figure 2-74 McDATA feature enablement login page

When you are logged in, the serial number and codes are entered on the page shown in Figure 2-75 and a feature key is generated.


Product Feature Enablement System - EUFRCSN - Mozilla Firefox
File
Edit
View
Go
Bookmarks
Tools
Help
https://mcdata.getkeys.com/pfes/ibm/sec/user
Go
IBM
Enable Feature(s)
Unit Information
My Profile
Logout
Upgrade your existing software!
Serial Number:
Transaction Code #1:
Transaction Code #2:
Transaction Code #3:
Transaction Code #4:
Transaction Code #5
Next
Software Upgrade
Click here to upgrade your existing software and obtain a new key
Done
mcdata.getkeys.com

Enable Feature(s)

Enter Product Information Step 1 of 3

To enable a feature, enter the Serial Number of the product and the transaction code(s) associated with the feature(s). Click **Next** to continue.

Copyright © 2005 McDATA Corporation. All rights reserved. Legal Notice

380 Interlocken Crescent, Broomfield, Colorado 80021
main: 720-558-8000, fax: 720.558.8999, e-mail:

Figure 2-75 McDATA transaction code entry page

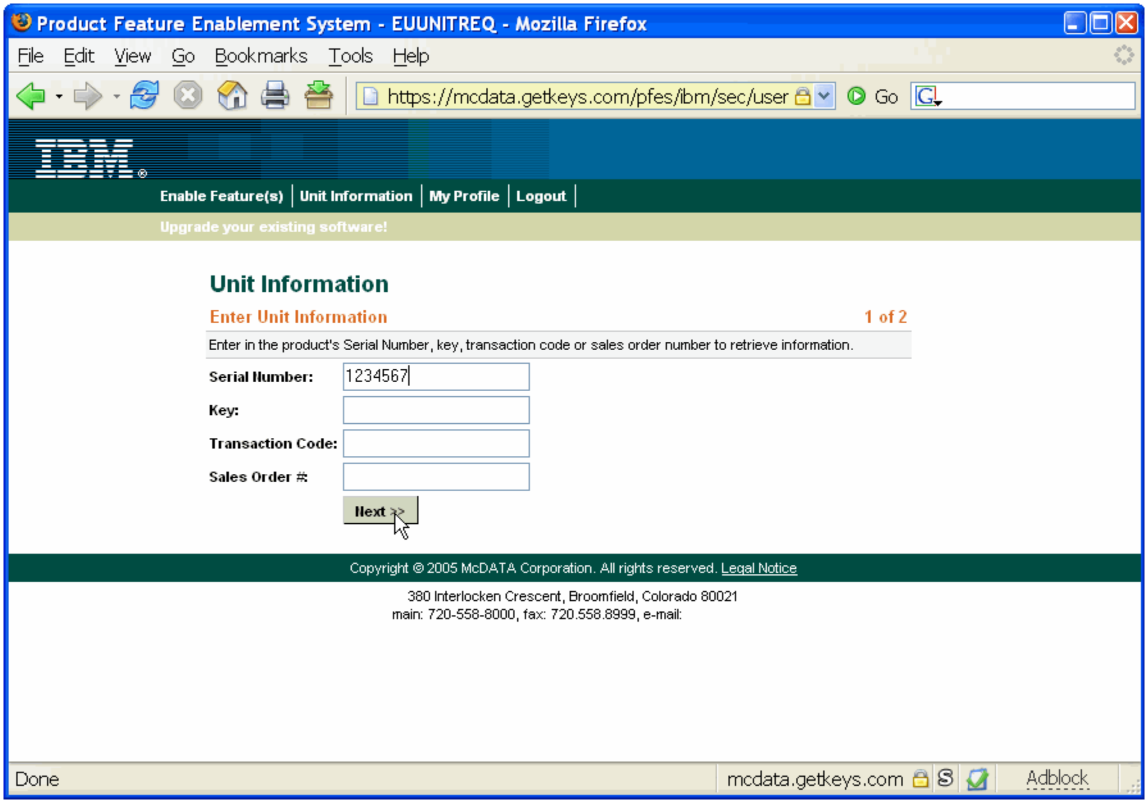
A feature key is a varying length string of alphanumeric characters consisting of both uppercase and lowercase (such as XxXx-XXxX-xxXX-xX).

Note: The total number of characters might vary. The key is case sensitive and it must be entered exactly as shown, including the dashes.

Encoded within the key are all the features that have been licensed for the product (Element Manager, OSMS, Open Trunking). If a new feature is purchased, a new key is generated to replace the existing one.

Key recovery

If for any reason you lose your transaction codes or feature key, you can recover them from the same Web site. Select the **Unit Information** link and enter the serial number of your product (1234567 in the example in Figure 2-76).


Product Feature Enablement System - EUUNITREQ - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://mcdata.getkeys.com/pfes/ibm/sec/user
Go
IBM
Enable Feature(s) | Unit Information | My Profile | Logout
Upgrade your existing software!
Next >>
Done
mcdata.getkeys.com
Adblock

Unit Information

Enter Unit Information 1 of 2

Enter in the product's Serial Number, key, transaction code or sales order number to retrieve information.

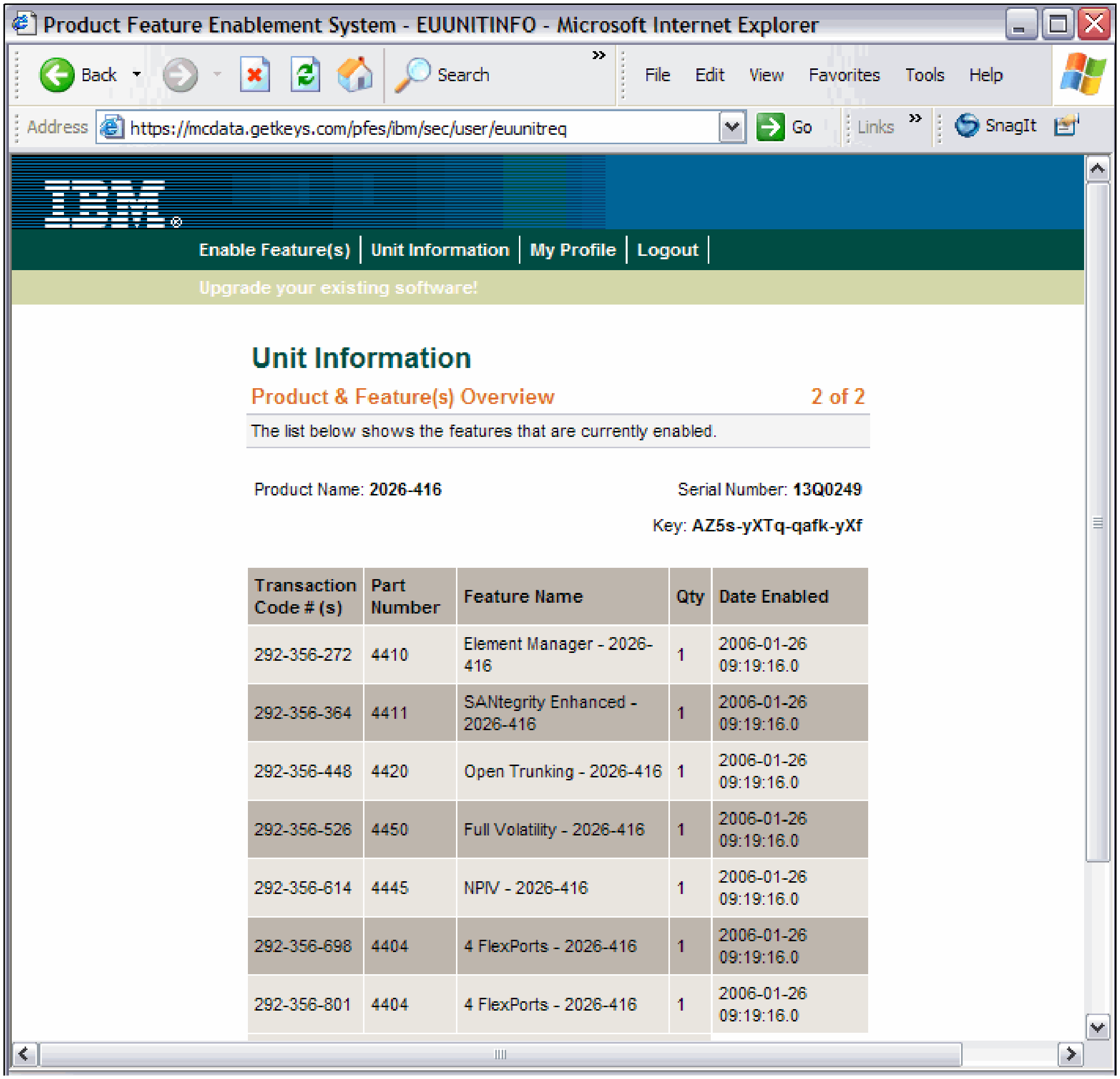
Serial Number: 1234567
Key:
Transaction Code:
Sales Order #:

Copyright © 2005 McDATA Corporation. All rights reserved. Legal Notice

380 Interlocken Crescent, Broomfield, Colorado 80021
main: 720-558-8000, fax: 720.558.8999, e-mail:

Figure 2-76 Unit information page

A page similar to that in Figure 2-77 shows all the transaction codes and the feature key for the product.


Product Feature Enablement System - EUUNITINFO - Microsoft Internet Explorer
Back
Search
File
Edit
View
Favorites
Tools
Help
Address
https://mcdata.getkeys.com/pfes/ibm/sec/user/euunitreq
Go
Links
SnagIt
IBM
Enable Feature(s)
Unit Information
My Profile
Logout
Upgrade your existing software!

Unit Information

Product & Feature(s) Overview 2 of 2

The list below shows the features that are currently enabled.

Product Name: **2026-416**

Serial Number: **13Q0249**

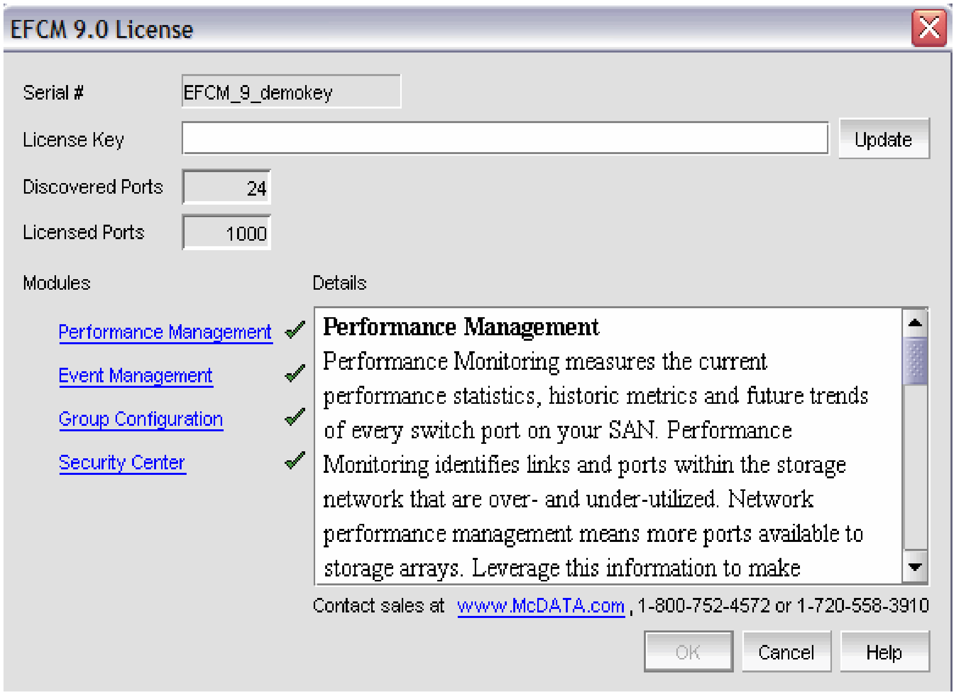
Key: **AZ5s-yXTq-qafk-yXf**

Transaction Code # (s)	Part Number	Feature Name	Qty	Date Enabled
292-356-272	4410	Element Manager - 2026-416	1	2006-01-26 09:19:16.0
292-356-364	4411	SANtegrity Enhanced - 2026-416	1	2006-01-26 09:19:16.0
292-356-448	4420	Open Trunking - 2026-416	1	2006-01-26 09:19:16.0
292-356-526	4450	Full Volatility - 2026-416	1	2006-01-26 09:19:16.0
292-356-614	4445	NPIV - 2026-416	1	2006-01-26 09:19:16.0
292-356-698	4404	4 FlexPorts - 2026-416	1	2006-01-26 09:19:16.0
292-356-801	4404	4 FlexPorts - 2026-416	1	2006-01-26 09:19:16.0

Figure 2-77 Product transaction codes and feature key

EFCM key installation

To view or update the licensed features of the EFCM server itself, select **Help** → **License** from the main window. The panel in Figure 2-78 displays (your EFCM serial number should also appear).


EFCM 9.0 License
Update
Modules
Details
Performance Management ✓
Event Management ✓
Group Configuration ✓
Security Center ✓
OK
Cancel
Help

Serial # EFCM_9_demokey

License Key

Discovered Ports 24

Licensed Ports 1000

Performance Management

Performance Monitoring measures the current performance statistics, historic metrics and future trends of every switch port on your SAN. Performance Monitoring identifies links and ports within the storage network that are over- and under-utilized. Network performance management means more ports available to storage arrays. Leverage this information to make

Contact sales at www.McDATA.com , 1-800-752-4572 or 1-720-558-3910

Figure 2-78 EFCM feature licensing

If you want to change the licensed features, enter a new license key and click **Update**. The rest of the window should update to reflect the new feature set. Finally, click **OK**.

Device key installation

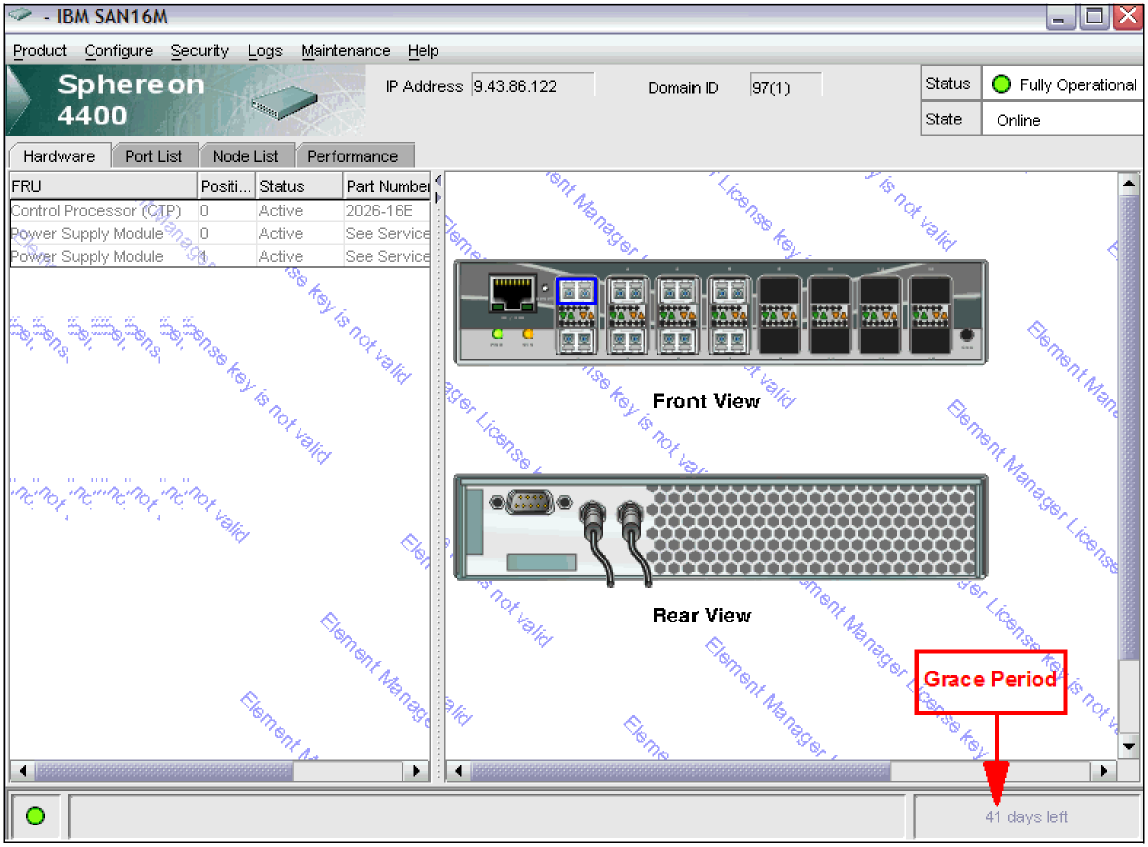
Keys can be installed via the CLI, the EFCM Basic Web GUI, or the Element Manager GUI.

Note: You might have to upgrade the product firmware, the EFCM server code, or both, before installing a key, if you are activating a recently available feature.

Attention: Enabling a feature is a non-disruptive process, but activating a key that removes a feature might be disruptive.

Device licensing with the EFCM Element Manager

When you first launch Element Manager for a device which has no licensed features installed, the window displays as shown in Figure 2-79. A new product provides a grace period (shown at the bottom right of the window) after which Element Manager no longer functions unless it has been licensed. When licensed, the diagonal blue background text disappears.


- IBM SAN16M
Product
Configure
Security
Logs
Maintenance
Help
Sphereon 4400
Hardware
Port List
Node List
Performance
Front View
Rear View
Grace Period
Element Manager License key is not valid

IP Address 9.43.86.122

Domain ID 97(1)

Status Fully Operational

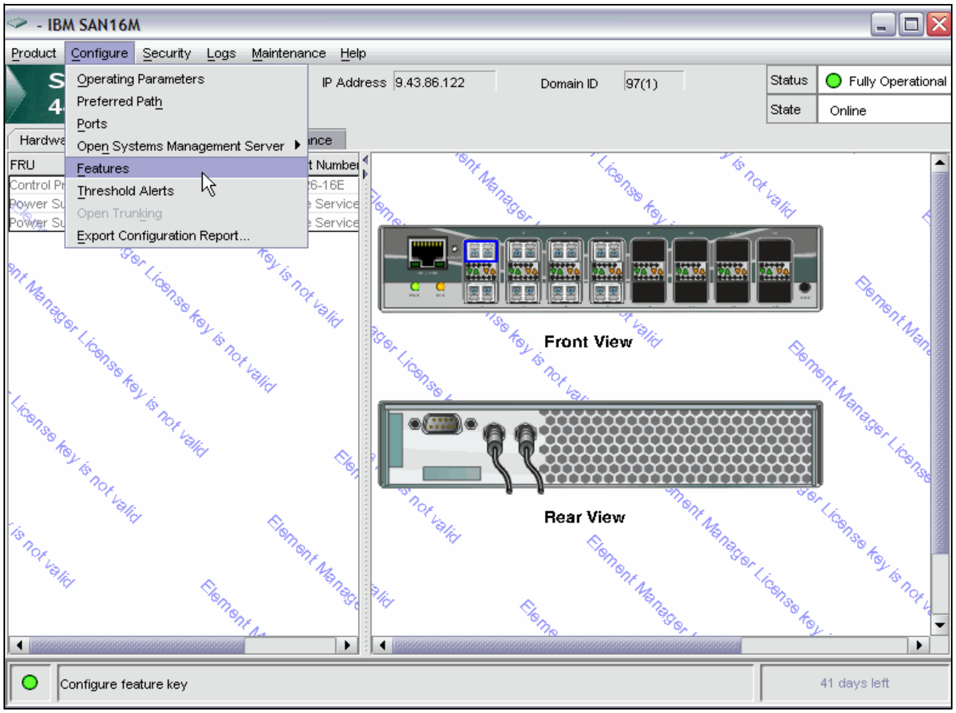
State Online

FRU	Positi...	Status	Part Number
Control Processor (CTP)	0	Active	2026-16E
Power Supply Module	0	Active	See Service
Power Supply Module	1	Active	See Service

41 days left

Figure 2-79 Unlicensed Element Manager

In the Element Manager window, select **Configure** → **Features...** as shown in Figure 2-80, and the current features are displayed.


- IBM SAN16M
Product
Configure
Security
Logs
Maintenance
Help
Operating Parameters
Preferred Path
Ports
Open Systems Management Server
Features
Threshold Alerts
Open Trunking
Export Configuration Report...
Hardwa
FRU
Front View
Rear View
Element Manager License key is not valid

IP Address 9.43.86.122

Domain ID 97(1)

Status Fully Operational

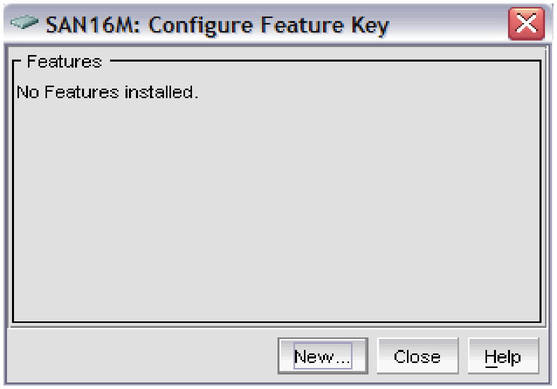
State Online

Configure feature key

41 days left

Figure 2-80 Element Manager feature selection

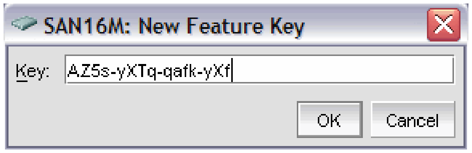
If this is a new product, the list is empty, as shown in Figure 2-81.Click the **New...** button.


SAN16M: Configure Feature Key
Features
New...
Close
Help

No Features installed.

Figure 2-81 Configured features

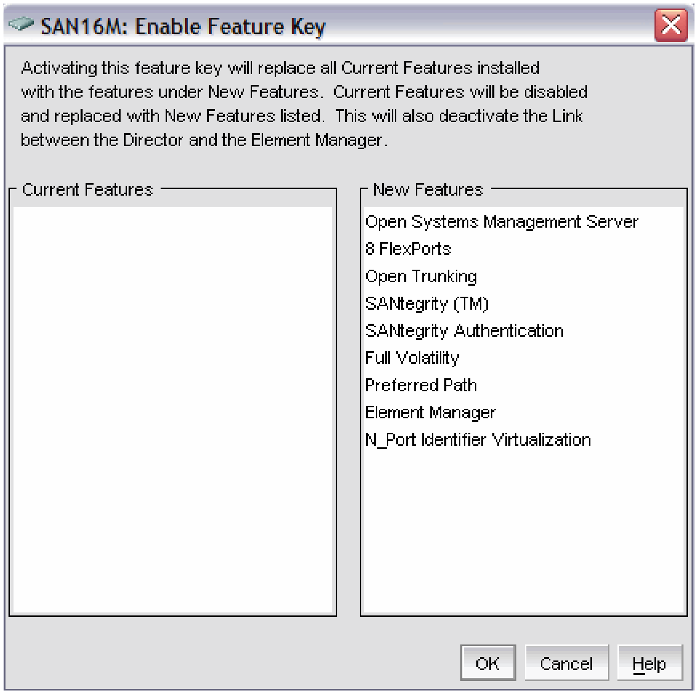
Enter the licence key in the window, as shown in Figure 2-82, and click **OK**.



Key: AZ5s-yXTq-qafk-yXf

Figure 2-82 Entering a new feature key

The window shown in Figure 2-83 should now appear, listing all the current and new features. Review these to ensure that the changes are correct and then click **OK**.



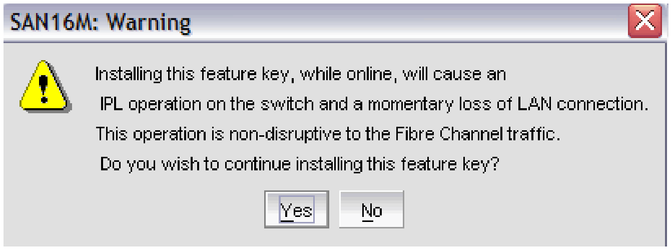
Activating this feature key will replace all Current Features installed with the features under New Features. Current Features will be disabled and replaced with New Features listed. This will also deactivate the Link between the Director and the Element Manager.

New Features:

Open Systems Management Server
8 FlexPorts
Open Trunking
SANtegrity (TM)
SANtegrity Authentication
Full Volatility
Preferred Path
Element Manager
N_Port Identifier Virtualization

Figure 2-83 Features being enabled

If the switch is online, then the warning shown in Figure 2-84 displays to remind you that feature activation will cause a switch IPL. This is non-disruptive to Fibre Channel traffic, so click **Yes** to proceed.


SAN16M: Warning
Yes
No

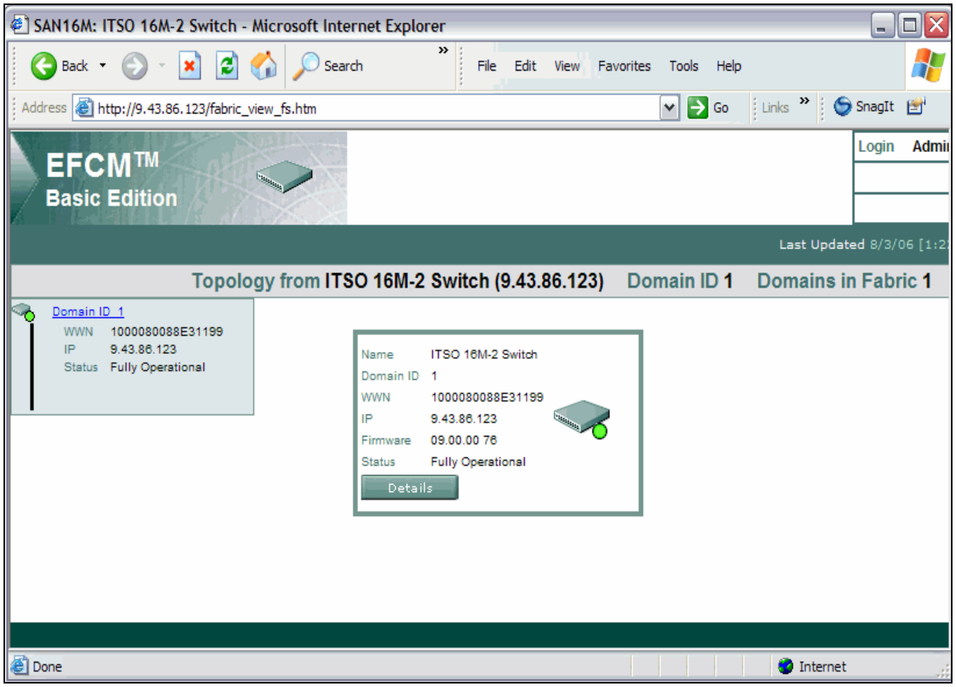
Installing this feature key, while online, will cause an IPL operation on the switch and a momentary loss of LAN connection. This operation is non-disruptive to the Fibre Channel traffic. Do you wish to continue installing this feature key?

Figure 2-84 Online activation warning

During the IPL, you might notice the EFCM temporarily losing contact with the switch.

Device licensing with EFCM Basic Web GUI

Start a Web browser and enter the address of the switch. Login and you should see a panel similar to that in Figure 2-85


SAN16M: ITSO 16M-2 Switch - Microsoft Internet Explorer
Back
Search
File
Edit
View
Favorites
Tools
Help
Address
Go
Links
SnagIt
EFCM™
Basic Edition
Login
Admi
Details
Done
Internet

http://9.43.86.123/fabric_view_fs.htm

Last Updated 8/3/06 [1:2

Topology from **ITSO 16M-2 Switch (9.43.86.123)** Domain ID **1** Domains in Fabric **1**

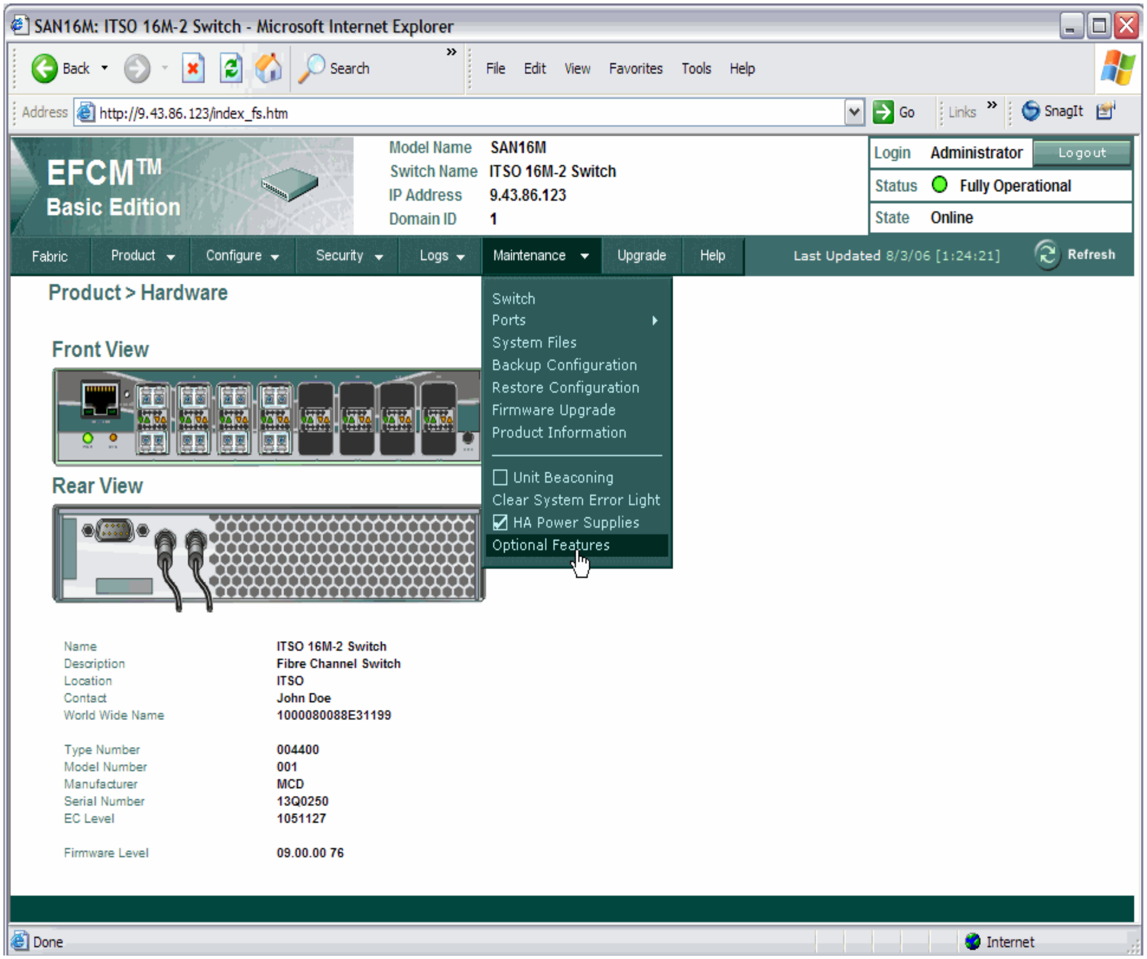
Domain ID 1

WWN	1000080088E31199
IP	9.43.86.123
Status	Fully Operational

Name	ITSO 16M-2 Switch
Domain ID	1
WWN	1000080088E31199
IP	9.43.86.123
Firmware	09.00.00 76
Status	Fully Operational

Figure 2-85 EFCM Basic fabric view

Click the **Switch Details** button and on the next window, click **Maintenance** → **Optional features**, as shown in Figure 2-86.

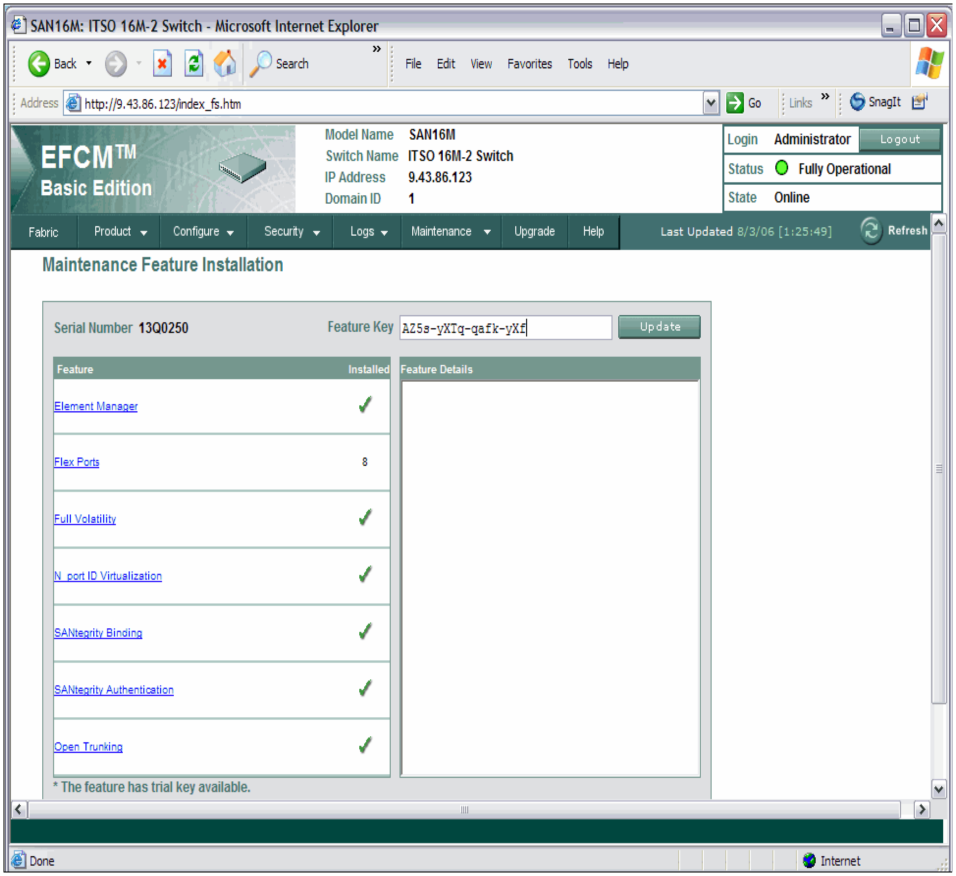

SAN16M: ITSO 16M-2 Switch - Microsoft Internet Explorer
Back
Search
File Edit View Favorites Tools Help
Address http://9.43.86.123/index_fs.htm
Go
Links
SnagIt
EFCM™ Basic Edition
Logout
Fabric
Product
Configure
Security
Logs
Maintenance
Upgrade
Help
Last Updated 8/3/06 [1:24:21]
Refresh
Switch
Ports
System Files
Backup Configuration
Restore Configuration
Firmware Upgrade
Product Information
☐ Unit Beaconing
Clear System Error Light
☑ HA Power Supplies
Optional Features
Product > Hardware
Front View
Rear View
Done
Internet

Model Name	SAN16M
Switch Name	ITSO 16M-2 Switch
IP Address	9.43.86.123
Domain ID	1
Login	Administrator
Status	Fully Operational
State	Online

Name	ITSO 16M-2 Switch
Description	Fibre Channel Switch
Location	ITSO
Contact	John Doe
World Wide Name	1000080088E31199
Type Number	004400
Model Number	001
Manufacturer	MCD
Serial Number	13Q0250
EC Level	1051127
Firmware Level	09.00.00 76

Figure 2-86 Installing features with EFCM Basic

Enter the new feature key as shown in Figure 2-87 and click **Update**.


SAN16M: ITSO 16M-2 Switch - Microsoft Internet Explorer
Back
Search
File
Edit
View
Favorites
Tools
Help
Address
http://9.43.86.123/index_fs.htm
Go
Links
SnagIt
EFCM™
Basic Edition
Logout
Fabric
Product
Configure
Security
Logs
Maintenance
Upgrade
Help
Refresh
Done
Internet

Model Name SAN16M
Switch Name ITSO 16M-2 Switch
IP Address 9.43.86.123
Domain ID 1

Login Administrator
Status Fully Operational
State Online

Last Updated 8/3/06 [1:25:49]

Maintenance Feature Installation

Serial Number 13Q0250
Feature Key AZ5s-yXTq-qafk-yXf
Update

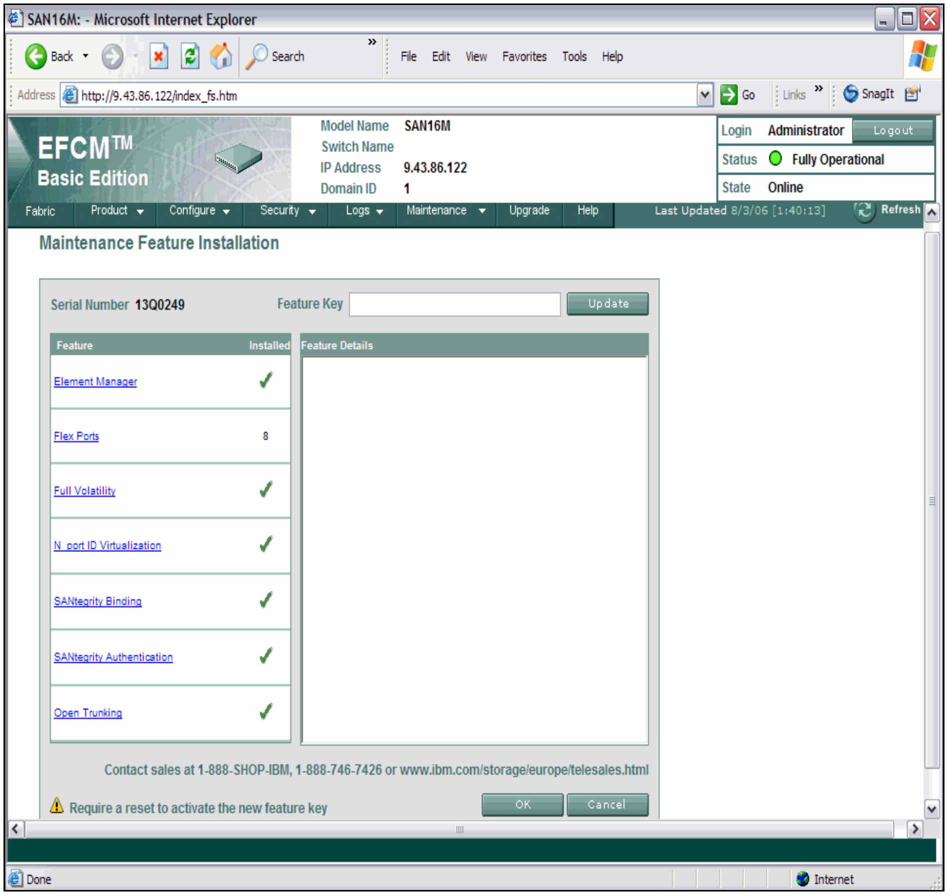
Feature	Installed
Element Manager	✓
Flex Ports	8
Full Volatility	✓
N_port ID Virtualization	✓
SANtegrity Binding	✓
SANtegrity Authentication	✓
Open Trunking	✓

Feature Details

* The feature has trial key available.

Figure 2-87 EFCM Basic feature key entry

A window like the one in Figure 2-88 is shown once the feature key is installed; notice the comment at the bottom, which requires you to IPL the switch for the change to take effect. Select the **OK** button to IPL.


SAN16M: - Microsoft Internet Explorer
Back
Search
File
Edit
View
Favorites
Tools
Help
Address
http://9.43.86.122/index_fs.htm
Go
Links
SnagIt
EFCM™
Basic Edition
Logout
Fabric
Product
Configure
Security
Logs
Maintenance
Upgrade
Help
Refresh
Update
OK
Cancel
Done
Internet

Model Name SAN16M
Switch Name
IP Address 9.43.86.122
Domain ID 1

Login Administrator
Status Fully Operational
State Online

Last Updated 8/3/06 [1:40:13]

Maintenance Feature Installation

Serial Number 13Q0249

Feature Key

Feature	Installed
Element Manager	✓
Flex Ports	8
Full Volatility	✓
N_port ID Virtualization	✓
SANtegrity Binding	✓
SANtegrity Authentication	✓
Open Trunking	✓

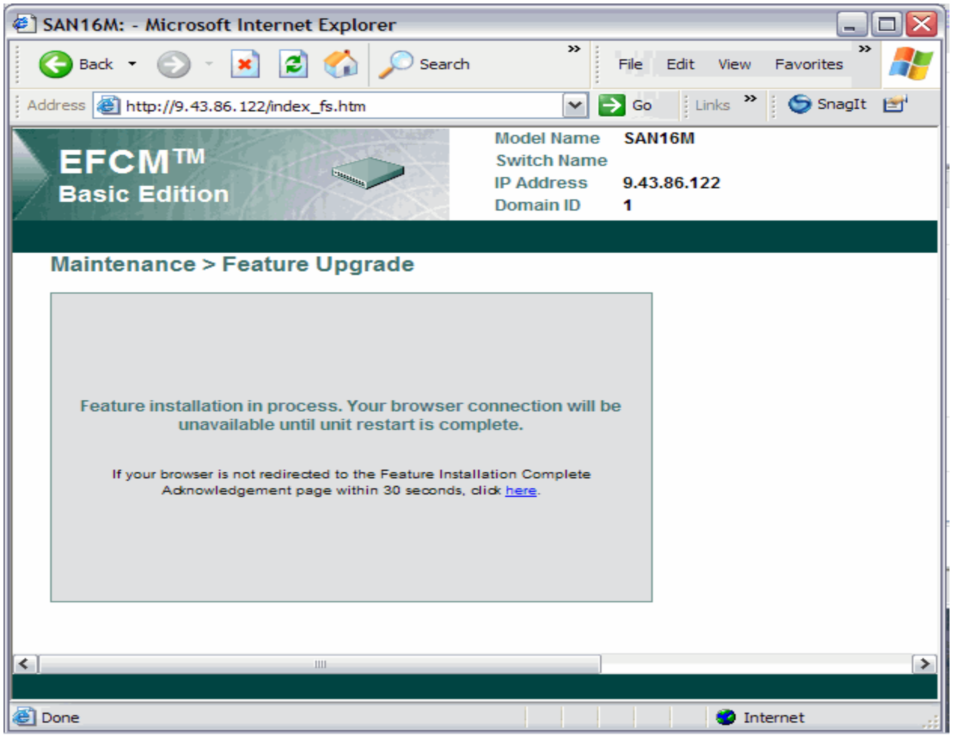
Feature Details

Contact sales at 1-888-SHOP-IBM, 1-888-746-7426 or www.ibm.com/storage/europe/telesales.html

⚠ Require a reset to activate the new feature key

Figure 2-88 Feature installation completion.

A window like the one shown in Figure 2-89 is displayed during IPL.


SAN16M: - Microsoft Internet Explorer
Back
Search
File
Edit
View
Favorites
Address
http://9.43.86.122/index_fs.htm
Go
Links
SnagIt
EFCM™
Basic Edition
Done
Internet

Model Name SAN16M
Switch Name
IP Address 9.43.86.122
Domain ID 1

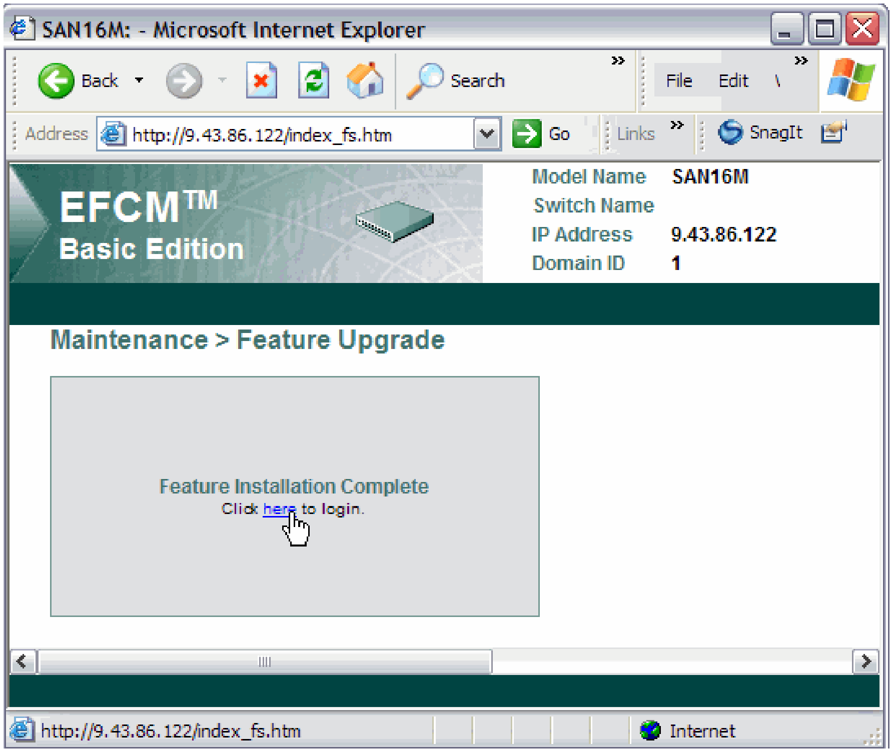
Maintenance > Feature Upgrade

Feature installation in process. Your browser connection will be unavailable until unit restart is complete.

If your browser is not redirected to the Feature Installation Complete Acknowledgement page within 30 seconds, click here.

Figure 2-89 Switch IPL in progress.

Upon completion of the feature upgrade, you have to log into the switch via the window shown in Figure 2-90.



http://9.43.86.122/index_fs.htm

Model Name SAN16M
Switch Name
IP Address 9.43.86.122
Domain ID 1

Maintenance > Feature Upgrade

Feature Installation Complete
Click here to login.

Figure 2-90 Feature Upgrade completion.

2.14.13 Obtaining software, firmware, and documentation

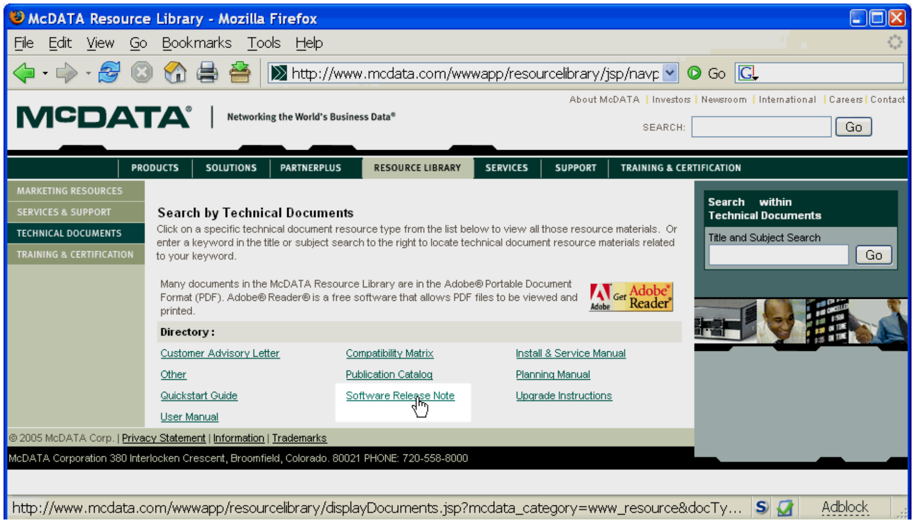
Before proceeding to download and activate any new firmware, or install new levels of EFCM software, it is a best practice to carefully read the firmware release notes to understand the implications and also to verify the fix list for any known problems.

The release notes (and other manuals) are available from the Technical Documents section of the McDATA Resource Library Web site (see Figure 2-91 on page 473):

`http://www.mcdata.com/resources/tdoc/index.html`

The following IBM Web site contains links to the latest interoperability matrixes for all m-type and McDATA switches sold by IBM. These contain notes on the recommended E/OS and EFCM levels.

`http://www-03.ibm.com/servers/storage/support/san/mcdatadownload.html`


McDATA Resource Library - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.mcdata.com/wwwapp/resourcelibrary/jsp/navp
Go
About McDATA | Investors | Newsroom | International | Careers | Contact
McDATA
Networking the World's Business Data®
SEARCH:
Go
PRODUCTS
SOLUTIONS
PARTNERPLUS
RESOURCE LIBRARY
SERVICES
SUPPORT
TRAINING & CERTIFICATION
MARKETING RESOURCES
SERVICES & SUPPORT
TECHNICAL DOCUMENTS
TRAINING & CERTIFICATION
Search within Technical Documents
Title and Subject Search
Go
Get Adobe Reader

Search by Technical Documents

Click on a specific technical document resource type from the list below to view all those resource materials. Or enter a keyword in the title or subject search to the right to locate technical document resource materials related to your keyword.

Many documents in the McDATA Resource Library are in the Adobe® Portable Document Format (PDF). Adobe® Reader® is a free software that allows PDF files to be viewed and printed.

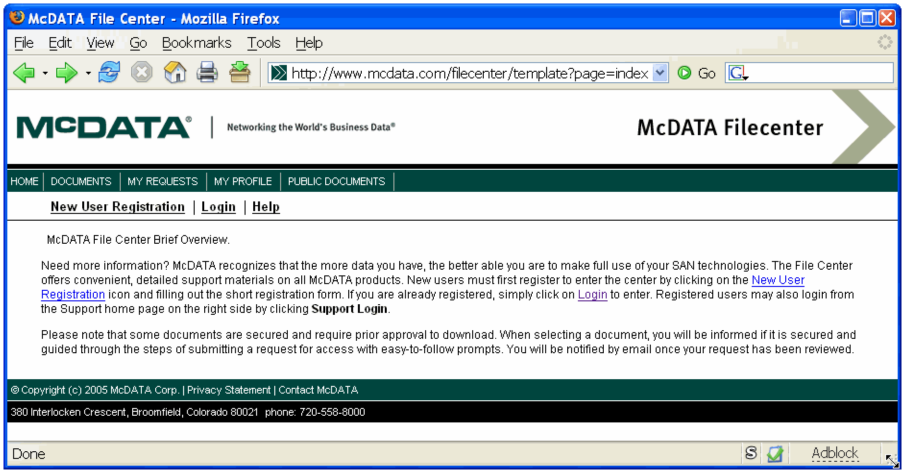
Directory:

Customer Advisory Letter
Compatibility Matrix
Install & Service Manual
Other
Publication Catalog
Planning Manual
Quickstart Guide
Software Release Note
Upgrade Instructions
User Manual
© 2005 McDATA Corp. | Privacy Statement | Information | Trademarks
McDATA Corporation 380 Interlocken Crescent, Broomfield, Colorado. 80021 PHONE: 720-558-8000
http://www.mcdata.com/wwwapp/resourcelibrary/displayDocuments.jsp?mcdata_category=www_resource&docTy...
Adblock

Figure 2-91 McDATA Resource Library for release notes

You must be registered to access the McDATA File Center Web site. This is free, and can be performed by clicking the **New User Registration** link shown in Figure 2-92 and available at:

http://www.mcdata.com/filecenter/template?page=index


McDATA File Center - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.mcdata.com/filecenter/template?page=index
Go
McDATA
Networking the World's Business Data®
McDATA Filecenter
HOME
DOCUMENTS
MY REQUESTS
MY PROFILE
PUBLIC DOCUMENTS
New User Registration | Login | Help

McDATA File Center Brief Overview.

Need more information? McDATA recognizes that the more data you have, the better able you are to make full use of your SAN technologies. The File Center offers convenient, detailed support materials on all McDATA products. New users must first register to enter the center by clicking on the New User Registration icon and filling out the short registration form. If you are already registered, simply click on Login to enter. Registered users may also login from the Support home page on the right side by clicking **Support Login**.

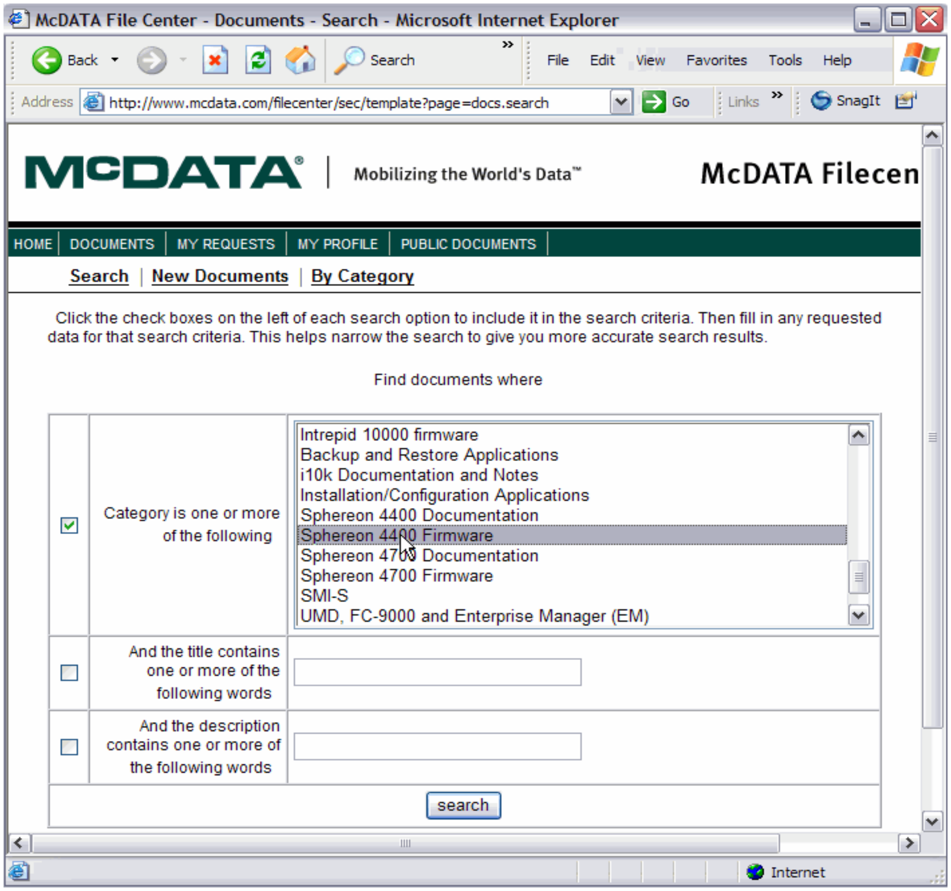
Please note that some documents are secured and require prior approval to download. When selecting a document, you will be informed if it is secured and guided through the steps of submitting a request for access with easy-to-follow prompts. You will be notified by email once your request has been reviewed.

© Copyright (c) 2005 McDATA Corp. | Privacy Statement | Contact McDATA
380 Interlocken Crescent, Broomfield, Colorado 80021 phone: 720-558-8000
Done
Adblock

Figure 2-92 McDATA File Center for firmware

Requests for firmware and software require the serial number of a registered product you own, and for which you have a valid warranty, and must be approved. Such approval can take a few hours, as it normally occurs during US working hours.

When logged onto the Web site, you select the **Documents** option. Figure 2-93 shows the window displayed where you are given the option to select the switch type for which you want to download the firmware or documentation. See Figure 2-1 for the conversion from McData to IBM machine types.


McDATA File Center - Documents - Search - Microsoft Internet Explorer
Back
Search
File
Edit
View
Favorites
Tools
Help
Address
Go
Links
SnagIt
MCDATA®
Mobilizing the World's Data™
McDATA Filecen
HOME
DOCUMENTS
MY REQUESTS
MY PROFILE
PUBLIC DOCUMENTS
Search
New Documents
By Category
search
Internet

Address: http://www.mcdata.com/filecenter/sec/template?page=docs.search

Click the check boxes on the left of each search option to include it in the search criteria. Then fill in any requested data for that search criteria. This helps narrow the search to give you more accurate search results.

Find documents where

☑ Category is one or more of the following

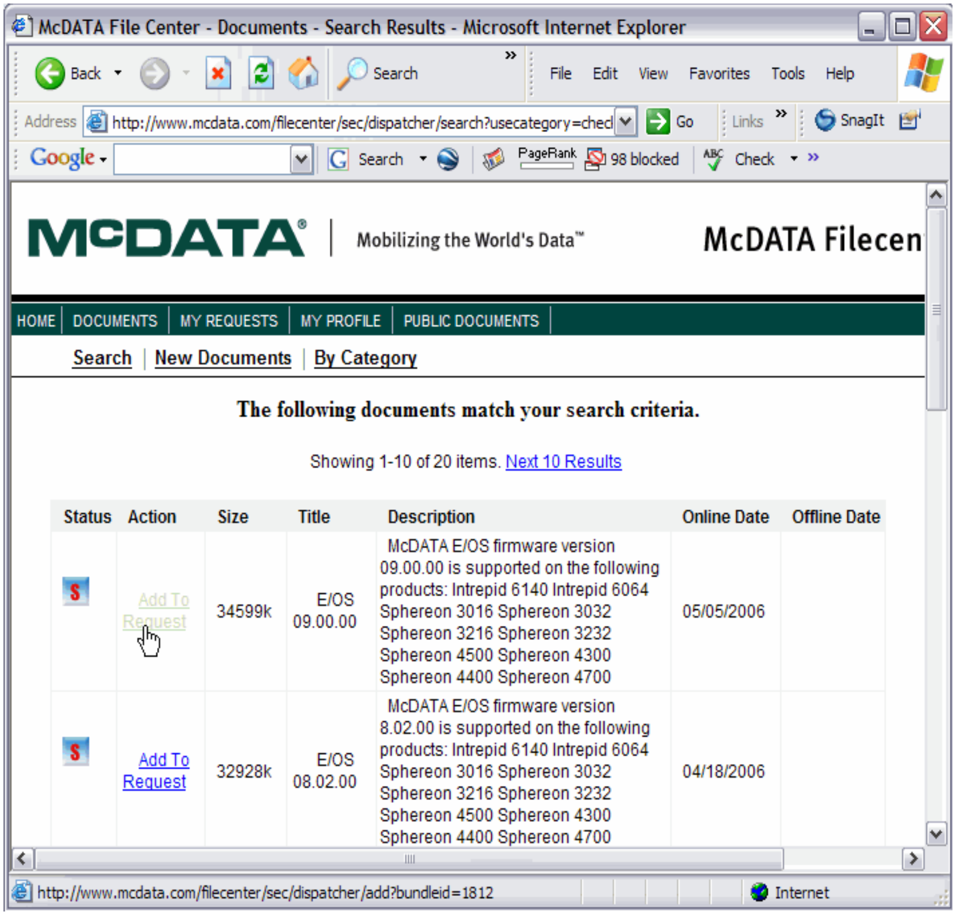
- Intrepid 10000 firmware
- Backup and Restore Applications
- i10k Documentation and Notes
- Installation/Configuration Applications
- Sphereon 4400 Documentation
- Sphereon 4400 Firmware
- Sphereon 4700 Documentation
- Sphereon 4700 Firmware
- SMI-S
- UMD, FC-9000 and Enterprise Manager (EM)

☐ And the title contains one or more of the following words

☐ And the description contains one or more of the following words

Figure 2-93 Firmware selection window

You now get a window, shown in Figure 2-94, where you select the version of firmware or documentation you want to download. Click the **Add To Request** link.


McDATA File Center - Documents - Search Results - Microsoft Internet Explorer
Back
Search
File
Edit
View
Favorites
Tools
Help
Address
http://www.mcdata.com/filecenter/sec/dispatcher/search?usecategory=chec
Go
Links
SnagIt
Google
Search
PageRank
98 blocked
Check
MCDATA
Mobilizing the World's Data™
McDATA Filecen
HOME
DOCUMENTS
MY REQUESTS
MY PROFILE
PUBLIC DOCUMENTS
Search
New Documents
By Category
http://www.mcdata.com/filecenter/sec/dispatcher/add?bundleid=1812
Internet

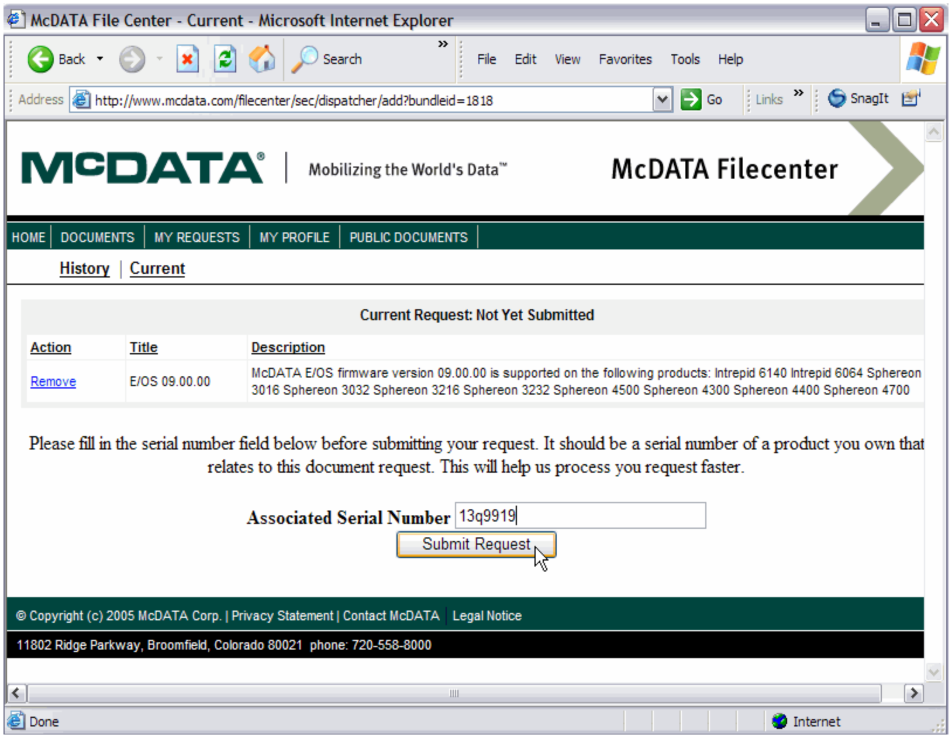
The following documents match your search criteria.

Showing 1-10 of 20 items. Next 10 Results

Status	Action	Size	Title	Description	Online Date	Offline Date
S	Add To Request	34599k	E/OS 09.00.00	McDATA E/OS firmware version 09.00.00 is supported on the following products: Intrepid 6140 Intrepid 6064 Sphereon 3016 Sphereon 3032 Sphereon 3216 Sphereon 3232 Sphereon 4500 Sphereon 4300 Sphereon 4400 Sphereon 4700	05/05/2006	
S	Add To Request	32928k	E/OS 08.02.00	McDATA E/OS firmware version 8.02.00 is supported on the following products: Intrepid 6140 Intrepid 6064 Sphereon 3016 Sphereon 3032 Sphereon 3216 Sphereon 3232 Sphereon 4500 Sphereon 4300 Sphereon 4400 Sphereon 4700	04/18/2006	

Figure 2-94 Firmware selection

You now get a new window where you have to enter the serial number of the switch you want to download, insert the serial number, and click the **Submit Request** button as shown in Figure 2-95.


McDATA File Center - Current - Microsoft Internet Explorer
Back
Search
File
Edit
View
Favorites
Tools
Help
Address
Go
Links
SnagIt
Mobilizing the World's Data™
McDATA Filecenter
HOME
DOCUMENTS
MY REQUESTS
MY PROFILE
PUBLIC DOCUMENTS
History
Current
Submit Request
Done
Internet

Address: http://www.mcdata.com/filecenter/sec/dispatcher/add?bundleid=1818

Current Request: Not Yet Submitted

Action	Title	Description
Remove	E/OS 09.00.00	McDATA E/OS firmware version 09.00.00 is supported on the following products: Intrepid 6140 Intrepid 6064 Sphereon 3016 Sphereon 3032 Sphereon 3216 Sphereon 3232 Sphereon 4500 Sphereon 4300 Sphereon 4400 Sphereon 4700

Please fill in the serial number field below before submitting your request. It should be a serial number of a product you own that relates to this document request. This will help us process you request faster.

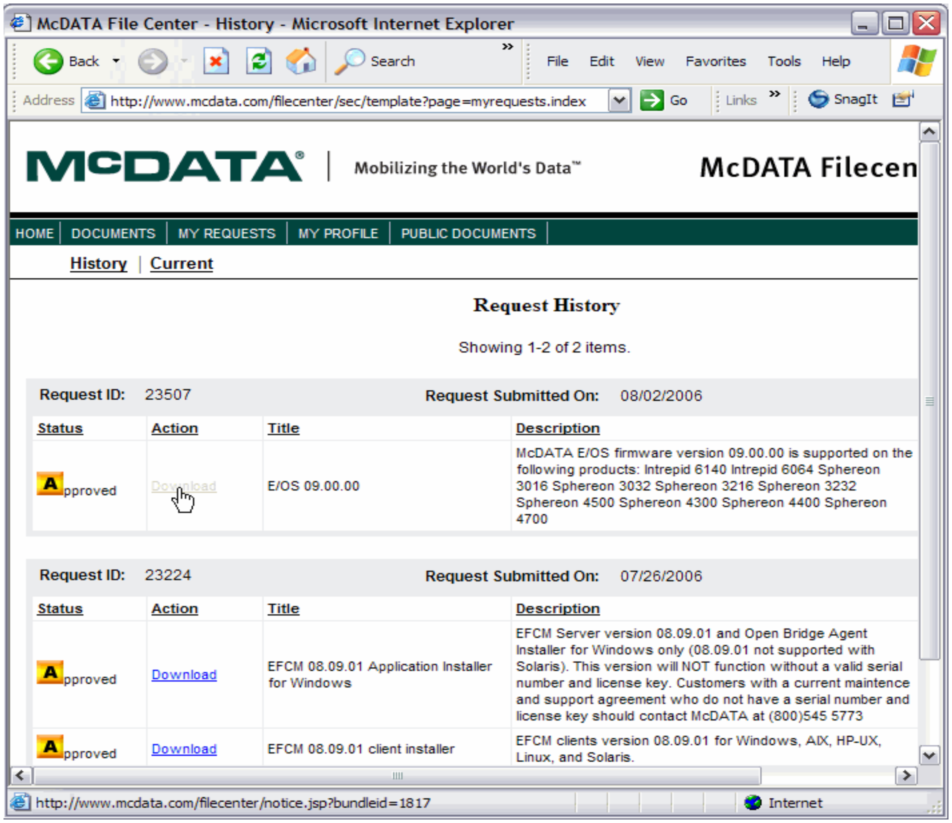
Associated Serial Number 13q9919

© Copyright (c) 2005 McDATA Corp. | Privacy Statement | Contact McDATA | Legal Notice

11802 Ridge Parkway, Broomfield, Colorado 80021 phone: 720-558-8000

Figure 2-95 Firmware Request

Some requests require authorization from McData, when you receive approval, via a Email sent to the Email address you used when you registered, return to the Web site, login and go to the *MY REQUESTS* section and you should see a list similar to that in Figure 2-96. Now click the **Download** link and save the file.


McDATA File Center - History - Microsoft Internet Explorer
Back
Search
File
Edit
View
Favorites
Tools
Help
Address
http://www.mcdata.com/filecenter/sec/template?page=myrequests.index
Go
Links
SnagIt
MCDATA
Mobilizing the World's Data™
McDATA Filecen
HOME
DOCUMENTS
MY REQUESTS
MY PROFILE
PUBLIC DOCUMENTS
History
Current
http://www.mcdata.com/filecenter/notice.jsp?bundleid=1817
Internet

Request History

Showing 1-2 of 2 items.

Request ID: 23507 **Request Submitted On:** 08/02/2006

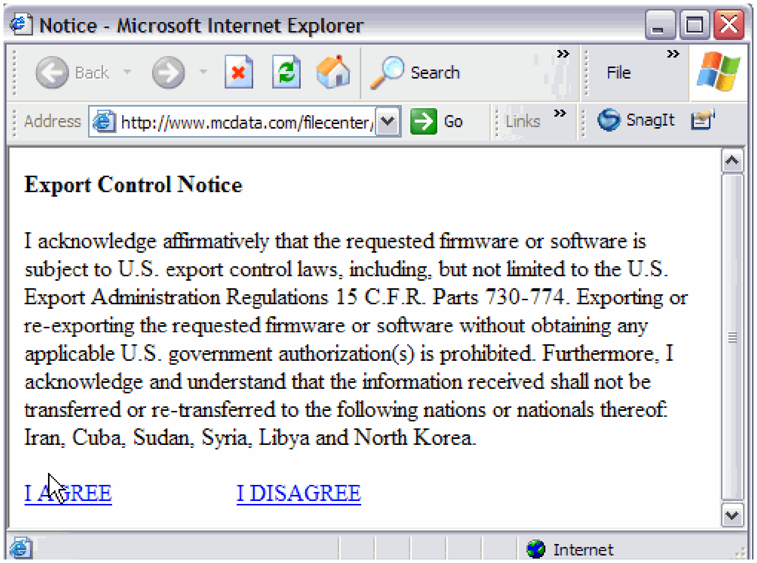
Status	Action	Title	Description
Approved	Download	E/OS 09.00.00	McDATA E/OS firmware version 09.00.00 is supported on the following products: Intrepid 6140 Intrepid 6064 Sphereon 3016 Sphereon 3032 Sphereon 3216 Sphereon 3232 Sphereon 4500 Sphereon 4300 Sphereon 4400 Sphereon 4700

Request ID: 23224 **Request Submitted On:** 07/26/2006

Status	Action	Title	Description
Approved	Download	EFCM 08.09.01 Application Installer for Windows	EFCM Server version 08.09.01 and Open Bridge Agent Installer for Windows only (08.09.01 not supported with Solaris). This version will NOT function without a valid serial number and license key. Customers with a current maintence and support agreement who do not have a serial number and license key should contact McDATA at (800)545 5773
Approved	Download	EFCM 08.09.01 client installer	EFCM clients version 08.09.01 for Windows, AIX, HP-UX, Linux, and Solaris.

Figure 2-96 McDATA File Center approved requests

Accept the licence agreement as shown in Figure 2-97 and complete the download.


Notice - Microsoft Internet Explorer
Back
Search
File
Address
http://www.mcdata.com/filecenter/
Go
Links
SnagIt
Internet

Export Control Notice

I acknowledge affirmatively that the requested firmware or software is subject to U.S. export control laws, including, but not limited to the U.S. Export Administration Regulations 15 C.F.R. Parts 730-774. Exporting or re-exporting the requested firmware or software without obtaining any applicable U.S. government authorization(s) is prohibited. Furthermore, I acknowledge and understand that the information received shall not be transferred or re-transferred to the following nations or nationals thereof: Iran, Cuba, Sudan, Syria, Libya and North Korea.

I AGREE I DISAGREE

Figure 2-97 Licence agreement.

Full details of this procedure are provided in the relevant product's *Installation and Service Manual*, which you can download from the McData web site.

2.14.14 Firmware installation

Up to 32 firmware versions can be stored on the EFC management server hard drive and made available for download to a director or switch through the Element Manager application. Multiple firmware versions can also be stored on a browser PC hard drive and made available for download to the director from the EFCM Basic interface.

Although firmware upgrades are concurrent, we recommend that a maintenance window is scheduled in order to activate the new firmware and/or to negate any loss of connectivity issues that might occur, or be required, during the install.

The EFCM Element Manager is used to demonstrate the procedure to download the firmware to an IBM TotalStorage SAN16M-2 switch.

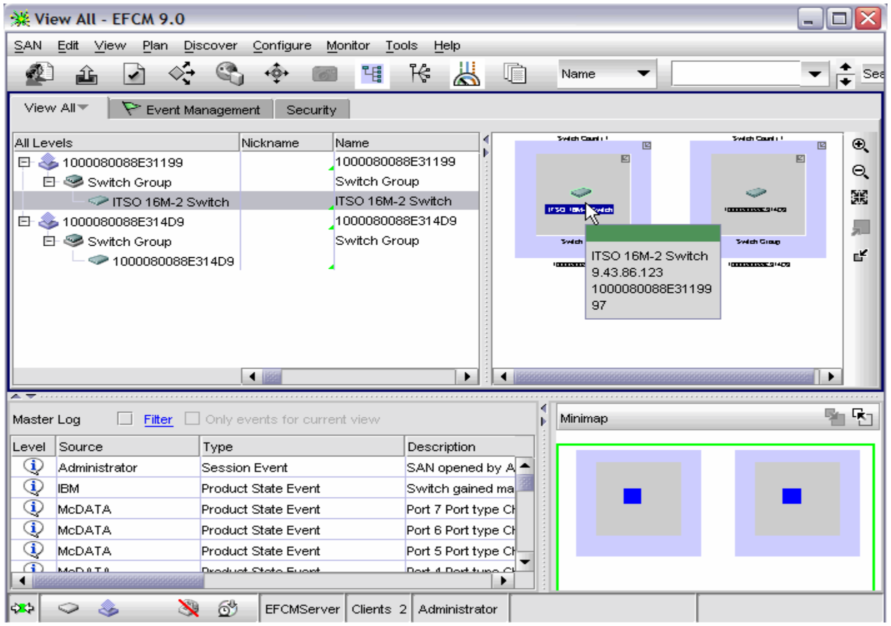
These are the steps that we took to update the firmware:

1. **Review the release notes:**

   Using the process described in “Obtaining software, firmware, and documentation” on page 472, download and review the release notes for the new E/OS. Also download the firmware file itself.

2. **Upgrade the EFCM software:**

   If necessary, download and upgrade the EFCM software on the EFC Server to the level required for the new E/OS code. This process is similar to that described in “EFCM server installation” on page 407. If you do this, remember to also upgrade the EFCM clients as their levels must match.


View All - EFCM 9.0
SAN
Edit
View
Plan
Discover
Configure
Monitor
Tools
Help
Name
View All
Event Management
Security
Master Log
Filter
Only events for current view
Minimap
EFCMServer
Clients 2
Administrator

All Levels	Nickname	Name
1000080088E31199		1000080088E31199
Switch Group		Switch Group
ITSO 16M-2 Switch		ITSO 16M-2 Switch
1000080088E314D9		1000080088E314D9
Switch Group		Switch Group
1000080088E314D9		

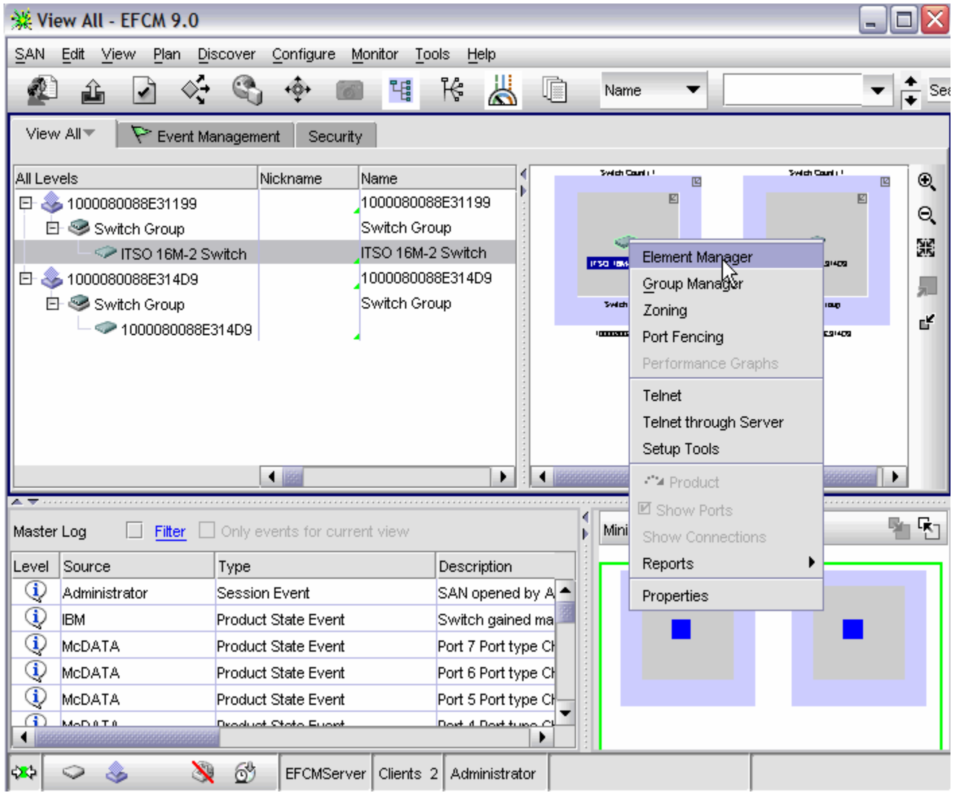
ITSO 16M-2 Switch
9.43.86.123
1000080088E31199
97

Level	Source	Type	Description
ⓘ	Administrator	Session Event	SAN opened by A
ⓘ	IBM	Product State Event	Switch gained ma
ⓘ	McDATA	Product State Event	Port 7 Port type Ch
ⓘ	McDATA	Product State Event	Port 6 Port type Ch
ⓘ	McDATA	Product State Event	Port 5 Port type Ch

Figure 2-98 Element Manager launch icon

3. **Launch the Element Manager for the switch:**

   In addition to double-clicking the product icon to open the Element Manager as we did before, we could also select the product icon and click the launch Element Manager icon as shown in Figure 2-98, or right-click the product in the EFCM view and choose **Element Manager** from the menu as shown in Figure 2-99.


View All - EFCM 9.0
SAN Edit View Plan Discover Configure Monitor Tools Help
Name
View All
Event Management
Security
All Levels
Nickname
Name
1000080088E31199
Switch Group
ITSO 16M-2 Switch
1000080088E314D9
Switch Group
1000080088E314D9
Element Manager
Group Manager
Zoning
Port Fencing
Performance Graphs
Telnet
Telnet through Server
Setup Tools
Product
Show Ports
Show Connections
Reports
Properties
Master Log
Filter
Only events for current view
EFCMServer
Clients 2
Administrator

Level	Source	Type	Description
ⓘ	Administrator	Session Event	SAN opened by A
ⓘ	IBM	Product State Event	Switch gained ma
ⓘ	McDATA	Product State Event	Port 7 Port type Cl
ⓘ	McDATA	Product State Event	Port 6 Port type Cl
ⓘ	McDATA	Product State Event	Port 5 Port type Cl

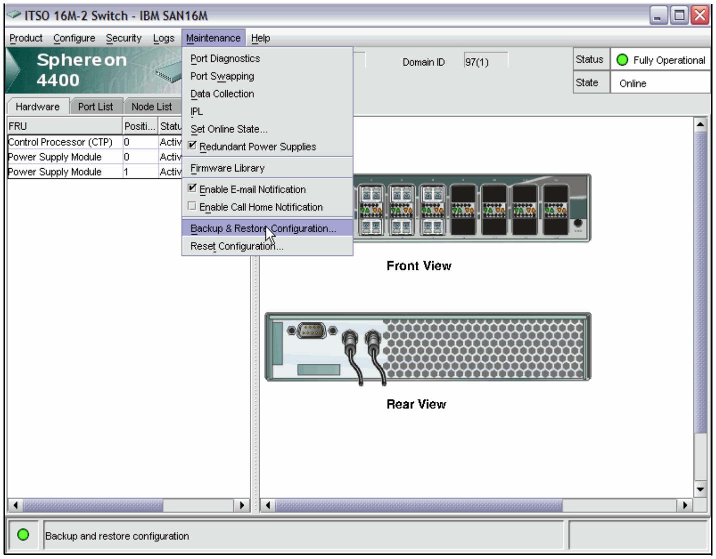
Figure 2-99 Invoking Element Manager with right-click

4. **Backup configuration:**

   This step enables you to revert to the old configuration, in case of configuration loss or corruption issues due to a CTP hang or incomplete firmware download, and is primarily for single-CTP switches.

   The EFC Server uses the Element Manager application to back up and restore the configuration data stored in the nonvolatile random-access memory (NV-RAM) on a director or switch CTP card to the EFC Manager data directory. The location and file name of the saved configuration cannot be modified, and only a single copy is kept. It only allows you to restore the configuration to an offline switch with the same IP address.

   From the Element Manager menu, select **Maintenance** → **Backup & Restore Configuration...** as shown in Figure 2-100.



ITSO 16M-2 Switch - IBM SAN16M

Domain ID 97(1)

Status: Fully Operational

State: Online

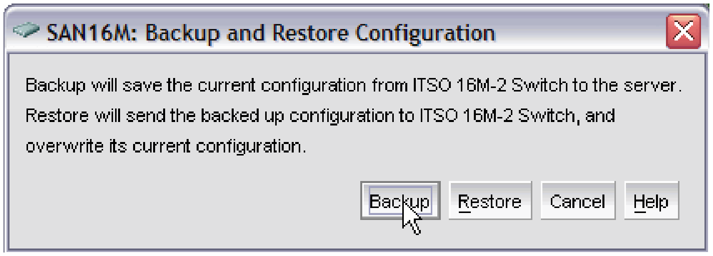
FRU	Positi...	Statu
Control Processor (CTP)	0	Activ
Power Supply Module	0	Activ
Power Supply Module	1	Activ

Backup and restore configuration

Product
Configure
Security
Logs
Maintenance
Help
Sphereon 4400
Hardware
Port List
Node List
Port Diagnostics
Port Swapping
Data Collection
IPL
Set Online State...
☑ Redundant Power Supplies
Firmware Library
☑ Enable E-mail Notification
☐ Enable Call Home Notification
Backup & Restore Configuration...
Reset Configuration...
Front View
Rear View

Figure 2-100 Backup and restore selection.

Click the **Backup** button as shown in Figure 2-101.



Backup will save the current configuration from ITSO 16M-2 Switch to the server. Restore will send the backed up configuration to ITSO 16M-2 Switch, and overwrite its current configuration.

Figure 2-101 Backup and Restore Configuration menu

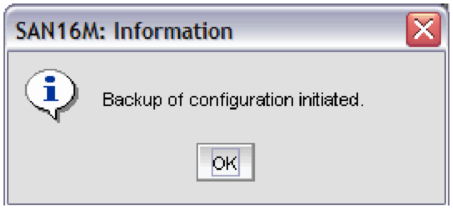
The following configurations are backed up to the EFC Server:

- Identification data (switch name, description, and location).
- Port configuration data (port names, blocked states, and extended distance settings).
- Operating parameters (BB_Credit, E_D_TOV, R_A_TOV, director priority, preferred domain ID, rerouting delay, and domain RSCNs).
- SNMP configuration (trap recipients, community names, and write authorizations).
- Zoning configuration (active zone set and default zone state).
- Alternate Control Prohibited settings.

SANtegrity Fabric Binding information is not backed up, but Switch Binding is.

Backup is immediately attempted when you click the **Backup** button. A dialog box confirms backup has been initiated as shown in Figure 2-102.

- A dialog box displays to confirm that the backup to the server is complete.
- If the backup fails, a dialog box displays to inform you that the backup to the server failed.

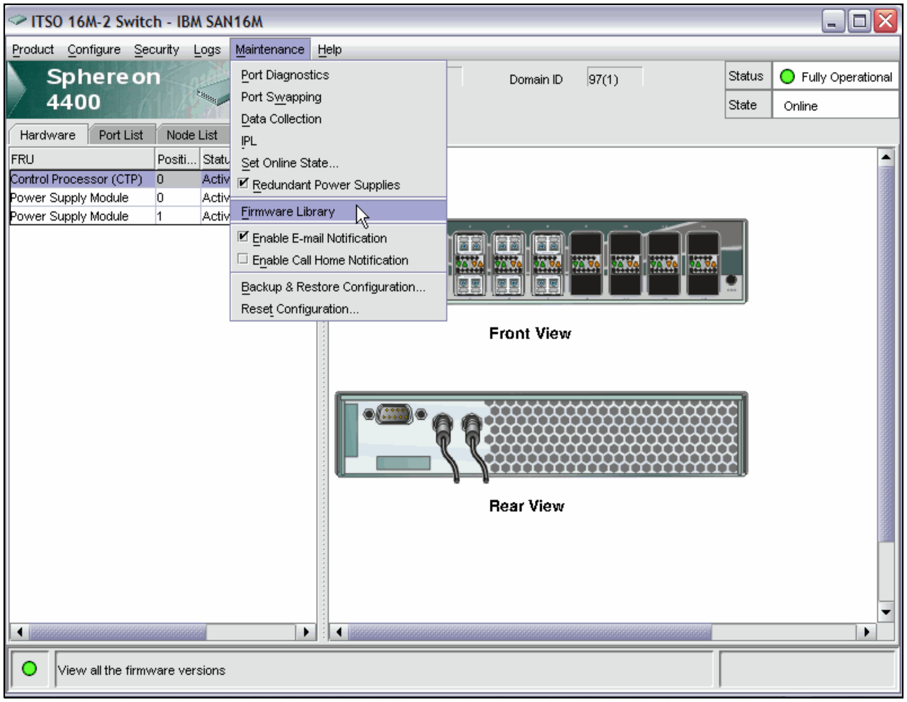


Backup of configuration initiated.

Figure 2-102 Backup initiation confirmation

Download the firmware image file and transfer it to the firmware library.

From the Element Manager menu, select **Maintenance** → **Firmware Library...** as shown in Figure 2-103.


ITSO 16M-2 Switch - IBM SAN16M
Product
Configure
Security
Logs
Maintenance
Help
Sphereon 4400
Port Diagnostics
Port Swapping
Data Collection
IPL
Set Online State...
☑ Redundant Power Supplies
Firmware Library
☑ Enable E-mail Notification
☐ Enable Call Home Notification
Backup & Restore Configuration...
Reset Configuration...
Hardware
Port List
Node List
Front View
Rear View

Domain ID 97(1)

Status: Fully Operational

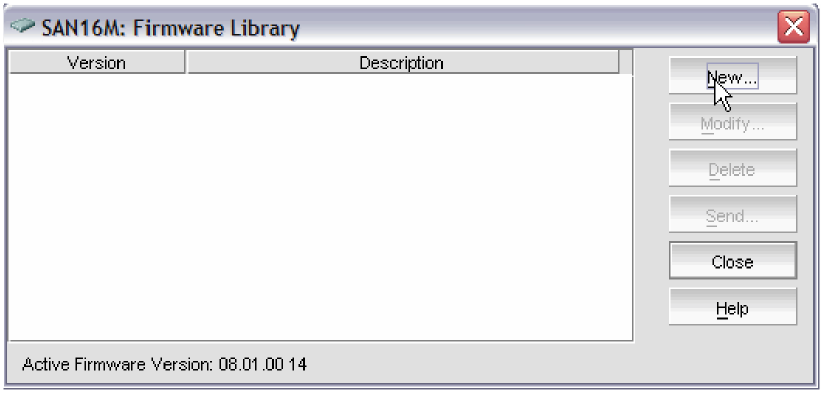
State: Online

FRU	Positi...	Statu
Control Processor (CTP)	0	Activ
Power Supply Module	0	Activ
Power Supply Module	1	Activ

View all the firmware versions

Figure 2-103 Firmware maintenance selection.

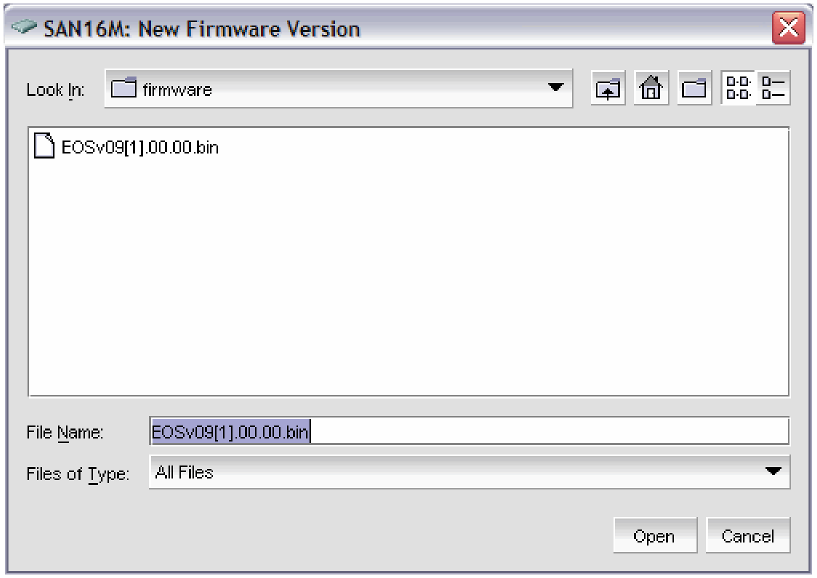
From the Element Manager menu, select **Maintenance** → **Firmware Library...** and then click the **New...** button as shown in Figure 2-104.


SAN16M: Firmware Library
Version
Description
New...
Modify...
Delete
Send...
Close
Help

Active Firmware Version: 08.01.00 14

Figure 2-104 EFCM Firmware Library

Now browse to the firmware image file and select **Open** as shown in Figure 2-105.

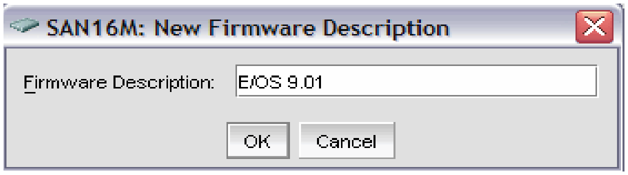

SAN16M: New Firmware Version
Look In:
firmware
EOSv09[1].00.00.bin
Open
Cancel

File Name: EOSv09[1].00.00.bin

Files of Type: All Files

Figure 2-105 New firmware version transferred to firmware library

Type a description and click the **OK** button to transfer the image file to the firmware library database. This is shown in Figure 2-106.


SAN16M: New Firmware Description
OK
Cancel

Firmware Description: E/OS 9.01

Figure 2-106 Firmware description

A progress bar, as shown in Figure 2-107, is displayed during the file transfer, which might take about a minute to complete.

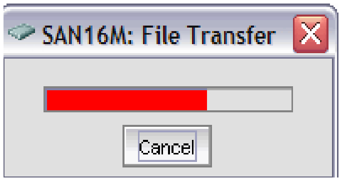
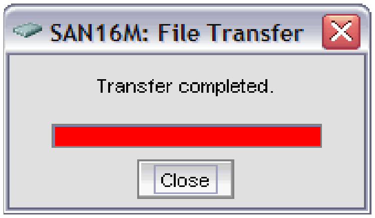

SAN16M: File Transfer
Cancel

Figure 2-107 Firmware file transfer in progress

This is replaced with the message box shown in Figure 2-108 when complete.

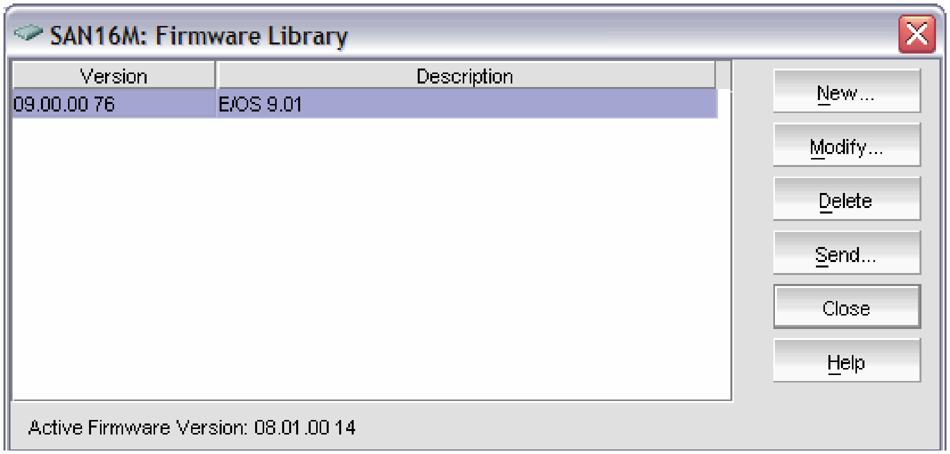

SAN16M: File Transfer

Transfer completed.

Close

Figure 2-108 Firmware transfer complete

As shown in Figure 2-109, the Firmware Library window now contains the new firmware.


SAN16M: Firmware Library
New...
Modify...
Delete
Send...
Close
Help

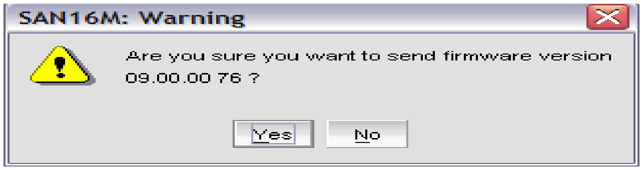
Version	Description
09.00.00 76	E/OS 9.01

Active Firmware Version: 08.01.00 14

Figure 2-109 Firmware library menu

5. **Download and activate the new firmware:**

   From the firmware library menu, select the firmware that was stored previously and click **Send...** You are prompted for confirmation to send the firmware, as shown in Figure 2-110.

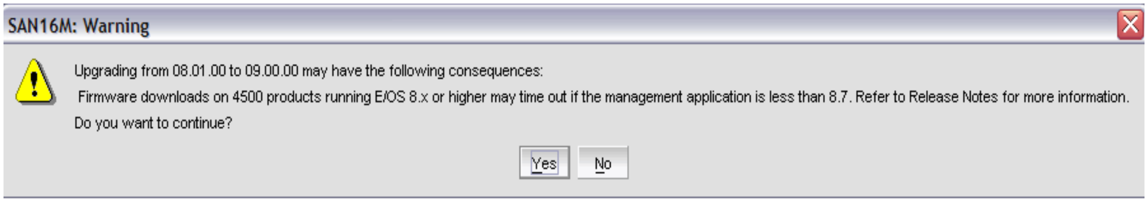

SAN16M: Warning

Are you sure you want to send firmware version 09.00.00 76 ?

Yes
No

Figure 2-110 Send firmware download confirmation prompt

The send function performs some verification checks before the download begins, and you might be shown a warning such as the one in Figure 2-111.


SAN16M: Warning

Upgrading from 08.01.00 to 09.00.00 may have the following consequences:

Firmware downloads on 4500 products running E/OS 8.x or higher may time out if the management application is less than 8.7. Refer to Release Notes for more information.

Do you want to continue?

Figure 2-111 Firmware activation warning prompt

If an error occurs, a message is displayed indicating the problem must be fixed before the firmware is downloaded. Conditions that could terminate the download process include these:

- There is a redundant CTP card failure (directors only).
- Another user is downloading firmware.
- The device-to-EFC server link is down.

Select **Yes** if all is satisfactory.

As the download proceeds, the progress bar shown on the left of Figure 2-112 is displayed, indicating the progress of the download. The bar reaches 50% when the last file is transmitted, at this point the device IPLs to activate the new code, as shown on the right of Figure 2-112.

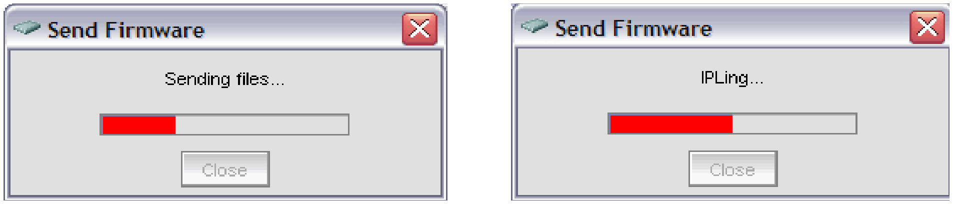
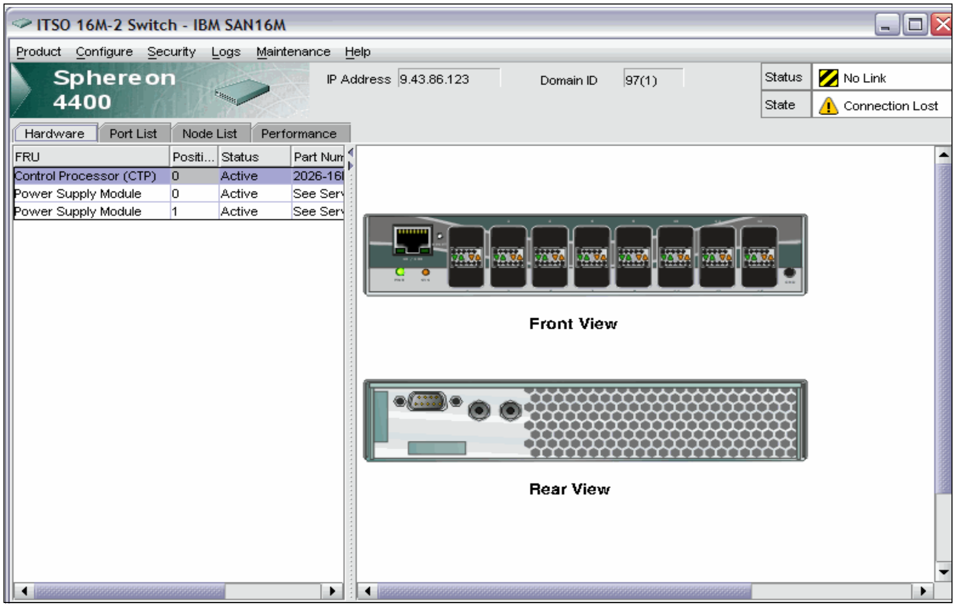


Figure 2-112 Sending firmware progress bars

Note: Sending firmware can take several minutes.

During the IPL, the device-to-EFC server link drops momentarily and the following indications occur at the Element Manager:

- As the network connection drops, the device status table turns yellow, the Status field displays `No Link`, and the Reason field displays a `Connection Lost` message, as shown in Figure 2-113.
- In the Product View, the device icon displays a grey square, indicating that the status is unknown.
- Illustrated FRUs in the Hardware View disappear, and appear again as the connection is re-established.


ITSO 16M-2 Switch - IBM SAN16M
Product
Configure
Security
Logs
Maintenance
Help
Sphereon 4400
Hardware
Port List
Node List
Performance
Front View
Rear View

IP Address 9.43.86.123

Domain ID 97(1)

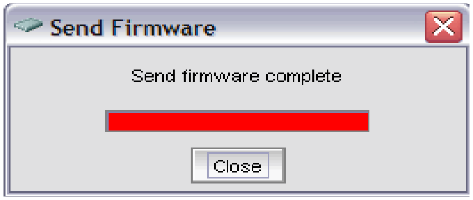
Status: No Link

State: Connection Lost

FRU	Positi...	Status	Part Num
Control Processor (CTP)	0	Active	2026-16
Power Supply Module	0	Active	See Ser
Power Supply Module	1	Active	See Ser

Figure 2-113 Network connection lost during IPL

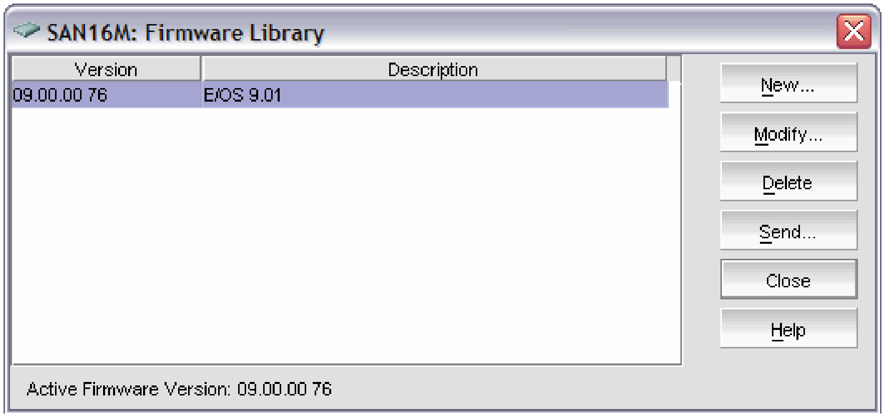
- After the IPL, the progress bar moves to 100% and the message in Figure 2-114 displays.


Send Firmware
Close

Send firmware complete

Figure 2-114 Firmware download complete

The firmware update is now complete, as indicated by the `Active Firmware Version` line at the bottom of the Firmware Library window shown in Figure 2-115.



SAN16M: Firmware Library

Version	Description
09.00.00 76	E/OS 9.01

Active Firmware Version: 09.00.00 76

Figure 2-115 New active firmware level

Normal service is now resumed.

Considerations regarding directors

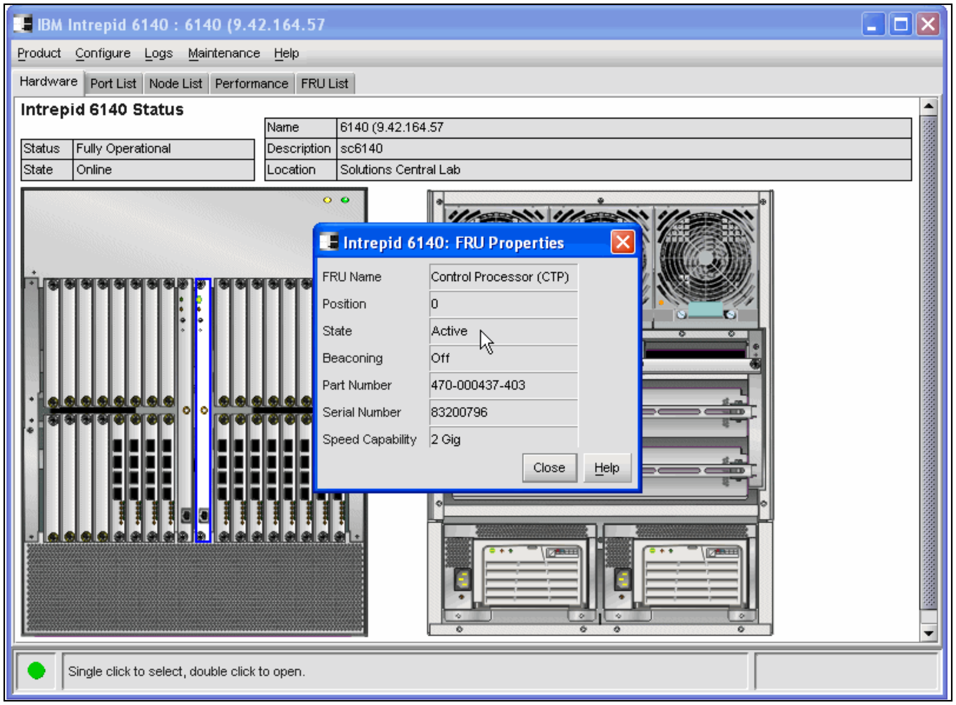
Switches only have one CTP, whereas directors have two. Hence a firmware upgrade on a director involves the extra steps of copying the firmware from one CTP to the other and activating the new firmware on the second CTP. This is all done automatically as part of sending the firmware, because whenever a CTP IPLs, it will ensure that the other CTP is at a matching firmware level.

After the first CTP IPLs, the message `Synchronizing CTPs` displays. This message remains as files are transmitted to the second CTP card and the progress bar travels across the window to 100%. When the download reaches 100%, the completion message shown in Figure 2-114 on page 487 is displayed.

If you have a policy of always running directors on a specific CTP card, you should verify that the correct card is now active, and perform a CTP switch if required. You can verify the active and backup CTP cards from the hardware menu of the SAN140M Element Manager view by double-clicking the CTP cards.

The FRU Properties window in Figure 2-116 shows that the CTP card in slot 0 is active.

Note: The same comments apply to the SAN256M director.


IBM Intrepid 6140 : 6140 (9.42.164.57
Product
Configure
Logs
Maintenance
Help
Hardware
Port List
Node List
Performance
FRU List
Intrepid 6140: FRU Properties
Close
Help

Intrepid 6140 Status

Status	Fully Operational
State	Online

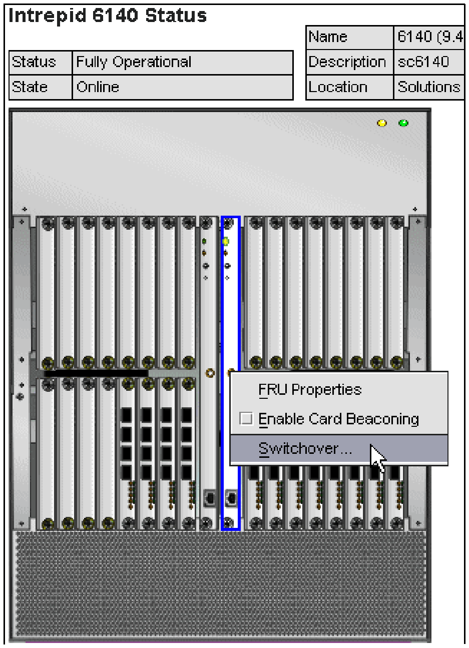
Name	6140 (9.42.164.57
Description	sc6140
Location	Solutions Central Lab

FRU Name	Control Processor (CTP)
Position	0
State	Active
Beaconing	Off
Part Number	470-000437-403
Serial Number	83200796
Speed Capability	2 Gig

Single click to select, double click to open.

Figure 2-116 CTP card status

If you have to perform a CTP switchover, right-click the active CTP card (CTP 0 in our example) and select the **Switchover...** option from the menu shown in Figure 2-117.


Intrepid 6140 Status

Status	Fully Operational
State	Online

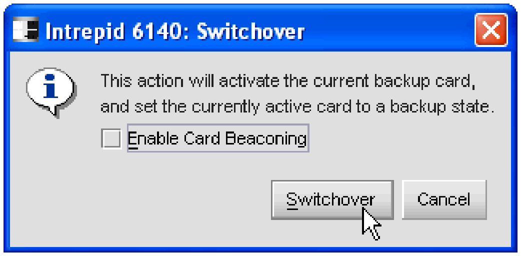
Name	6140 (9.4
Description	sc6140
Location	Solutions

FRU Properties
☐ Enable Card Beaconing
Switchover...

Figure 2-117 CTP switchover

In the Switchover window, click the **Switchover** button as shown in Figure 2-118 to switch operation to the backup CTP card. When switchover occurs, the green LED illuminates on the backup CTP card to indicate that it is now the active card.

Note: The director loses its Ethernet connection for a short period during the switchover process.


Intrepid 6140: Switchover

This action will activate the current backup card, and set the currently active card to a backup state.

☐ Enable Card Beaconing
Switchover
Cancel

Figure 2-118 CTP switchover button

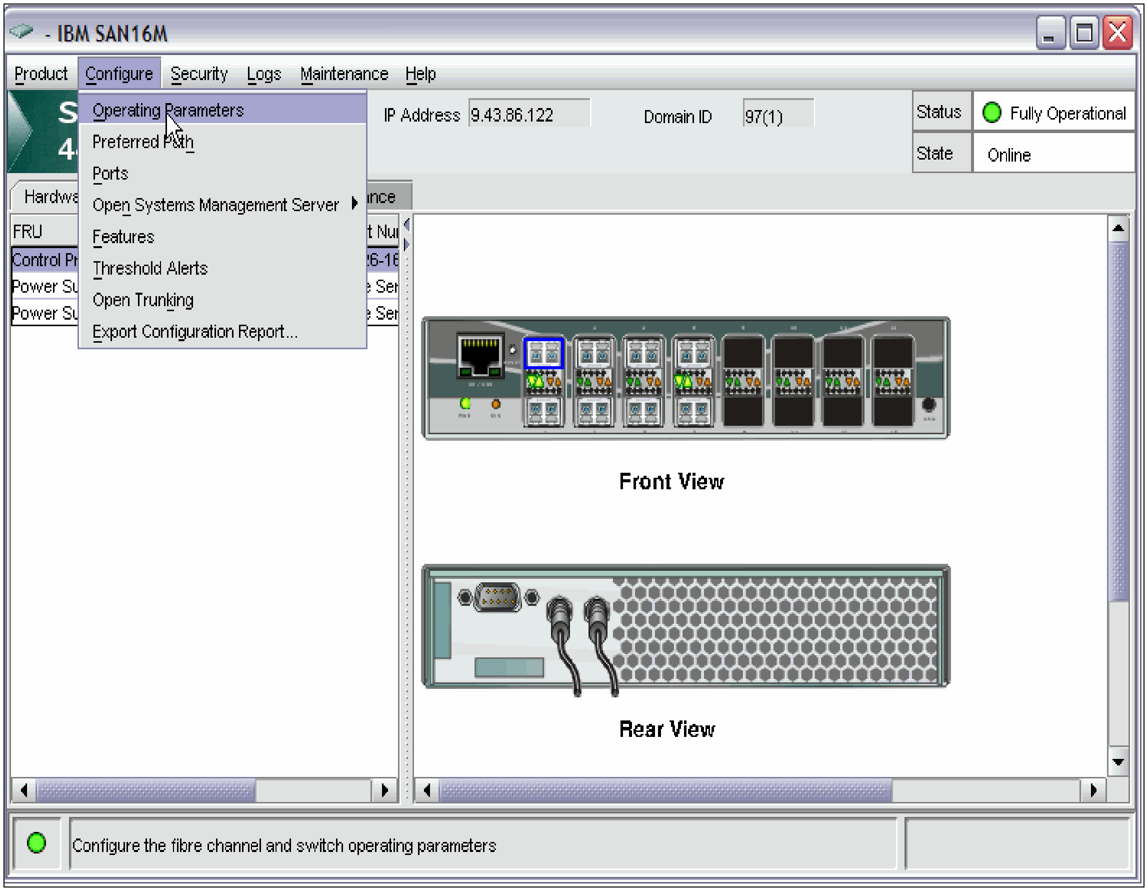
2.14.15 Initial switch configuration

In the topics that follow, we show some initial switch configuration steps. For the following examples, we use the Element Manager launched from EFCM, you could also use Element manager launched from EFCM Basic.

Configuring switch identification

Each switch and director should be assigned a name and description.

This is done using Element Manager by selecting **Configure** → **Operating Parameters** as shown in Figure 2-119.



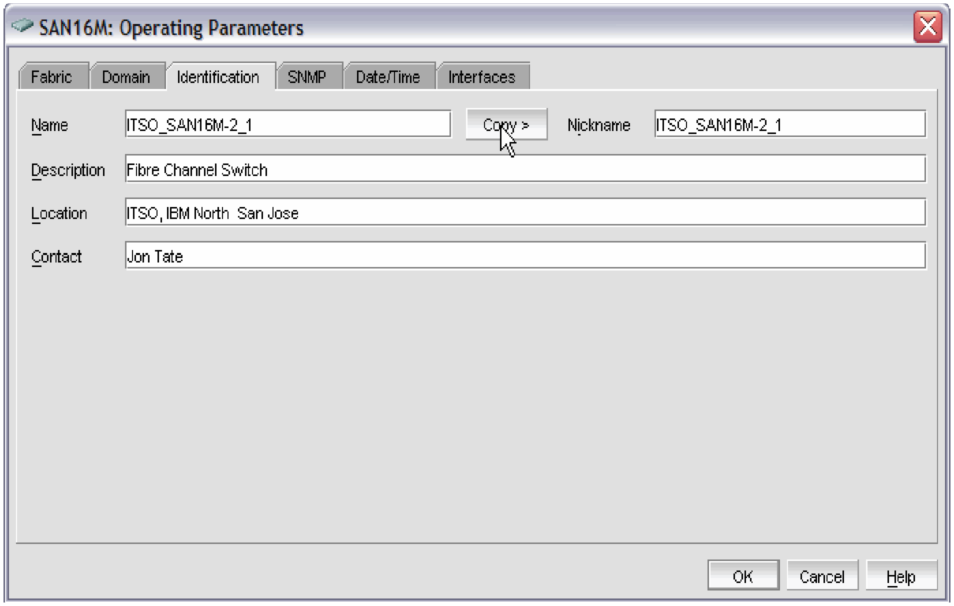
- IBM SAN16M
Product
Configure
Security
Logs
Maintenance
Help
Operating Parameters
Preferred Path
Ports
Open Systems Management Server
Features
Threshold Alerts
Open Trunking
Export Configuration Report...
IP Address
9.43.86.122
Domain ID
97(1)
Status
Fully Operational
State
Online
Hardwa
FRU
Control Pr
Power Su
Power Su
Front View
Rear View

Configure the fibre channel and switch operating parameters

Figure 2-119 Operating Parameters selection

Select the **Identification** tab and entering the appropriate information as shown in Figure 2-120. It is advisable to complete the location and contact fields, as they are included in e-mail alerts.

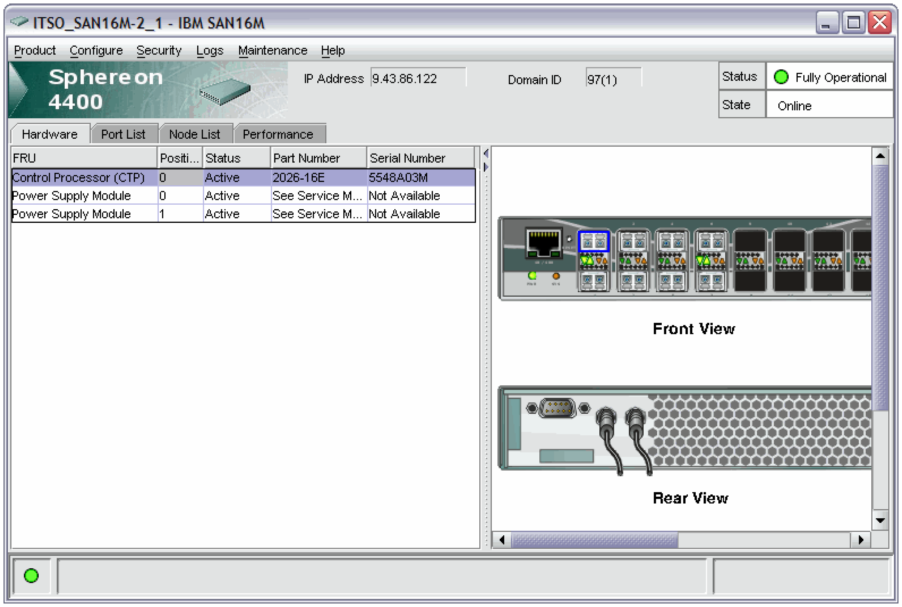
If you click the **Copy** button, the name is automatically created as a *nickname*. Click **OK** to commit the change.


SAN16M: Operating Parameters
Fabric
Domain
Identification
SNMP
Date/Time
Interfaces
Copy >
OK
Cancel
Help

Name: ITSO_SAN16M-2_1
Nickname: ITSO_SAN16M-2_1
Description: Fibre Channel Switch
Location: ITSO, IBM North San Jose
Contact: Jon Tate

Figure 2-120 Switch Operating Parameters dialog box

After activation, the display of the main window changes and places the name of the switch in the title bar, as shown in Figure 2-121. This information is used in various locations of the Element Manager to identify the selected switch or director.


ITSO_SAN16M-2_1 - IBM SAN16M
Product Configure Security Logs Maintenance Help
Sphereon 4400
Hardware
Port List
Node List
Performance
Front View
Rear View

IP Address 9.43.86.122
Domain ID 97(1)
Status ● Fully Operational
State Online

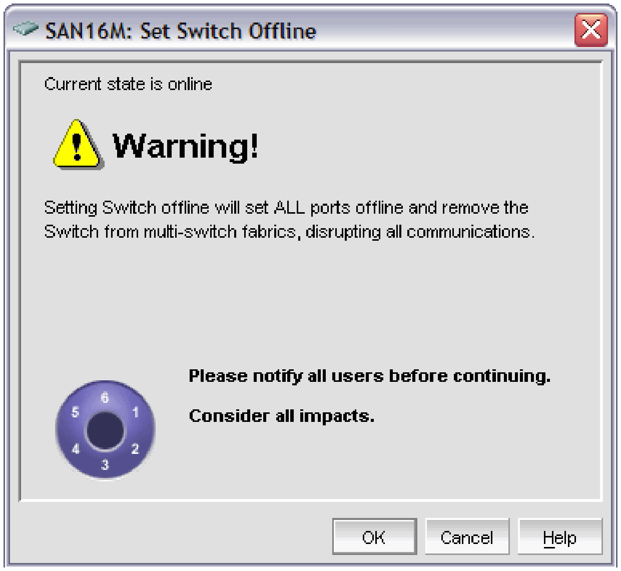
FRU	Positi...	Status	Part Number	Serial Number
Control Processor (CTP)	0	Active	2026-16E	5548A03M
Power Supply Module	0	Active	See Service M...	Not Available
Power Supply Module	1	Active	See Service M...	Not Available

Figure 2-121 SAN16M-2 hardware view changed

Taking the switch offline

Some of the following configuration changes can only be made if the switch is offline, so select **Maintenance** → **Set Online State.**

Because this is disruptive to the SAN, the warning message shown in Figure 2-122 displays and you have to click **OK** to confirm.


SAN16M: Set Switch Offline
OK
Cancel
Help

Current state is online

Warning!

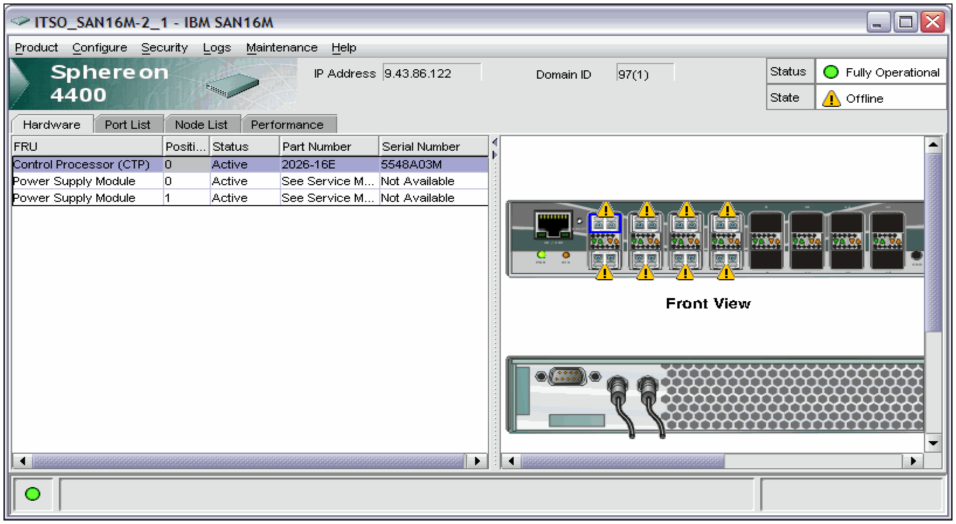
Setting Switch offline will set ALL ports offline and remove the Switch from multi-switch fabrics, disrupting all communications.

Please notify all users before continuing.

Consider all impacts.

Figure 2-122 Setting switch offline warning

After a few seconds, the Element Manager shows the switch state as *Offline*, as shown in Figure 2-123. The same method is used to bring the switch back online.


ITSO_SAN16M-2_1 - IBM SAN16M
Product
Configure
Security
Logs
Maintenance
Help
Sphereon 4400
Hardware
Port List
Node List
Performance
Front View

IP Address 9.43.86.122

Domain ID 97(1)

Status ● Fully Operational

State ⚠ Offline

FRU	Positi...	Status	Part Number	Serial Number
Control Processor (CTP)	0	Active	2026-16E	5548A03M
Power Supply Module	0	Active	See Service M...	Not Available
Power Supply Module	1	Active	See Service M...	Not Available

Figure 2-123 Switch offline state

Configuring switch operating parameters

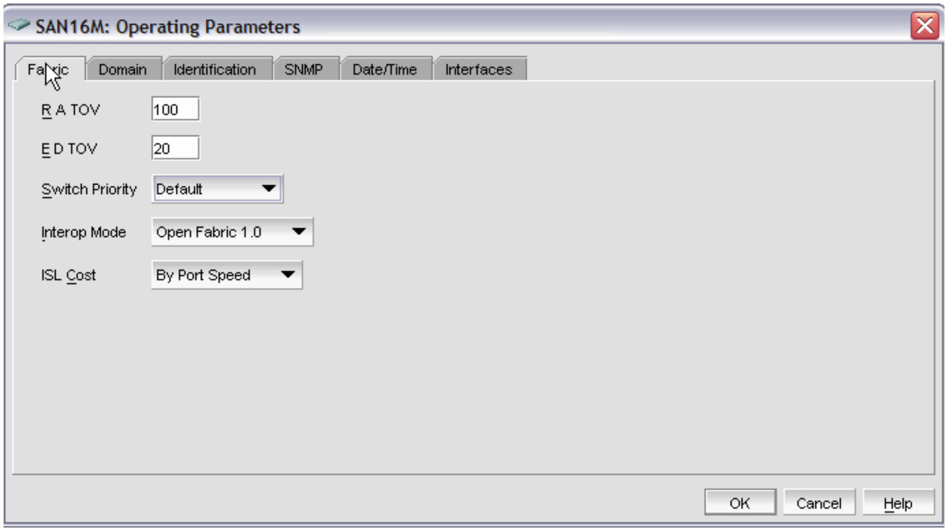
The following topics cover the settings that should be reviewed or changed when adding a new switch or director.

Priority and Interop Mode

In every multi-switch fabric, one switch has responsibility for the domain address manager functionality. This switch is known as the principal switch. It controls the allocation and distribution of the domain IDs for all connected switches in the fabric.

A switch can be manually set to be the principal switch, or it can be set to never be principal. This can be done in a core-to-edge environment, for example, where it makes sense for a core switch to normally be principal. If switches are set to the “default” priority, the one with the lowest numerical WWN value becomes the principal switch.

To change the Switch Priority, we use the Element Manager and select **Configure** → **Operating Parameters** as shown in Figure 2-120 on page 492 and then select the **Fabric tab...**, as shown here in Figure 2-124.



R A TOV: 100
E D TOV: 20
Switch Priority: Default
Interop Mode: Open Fabric 1.0
ISL Cost: By Port Speed

Figure 2-124 Element Manager: Configure Operating Parameters, Fabric

There must always be a principal switch in a fabric, so do *not* configure all your switches as *Never Principal* in the Switch Priority field.

Tip: For fabrics containing directors, you would normally want them to be principal, because they have higher availability. Hence you might set other switches as *Never Principal*, and leave the directors as *Principal or Default*.

Attention: When introducing new switches or directors into a fabric, be careful that you do not unintentionally change the fabric's principal switch. Before connecting ISLs from the new device to the existing ones, review the Switch Priority setting and compare the new switch's WWN with that of your current principal switch.

The use of the insistent domain ID feature can protect against this situation.

This is also where you can change the **Interop Mode** of the switch between *Open Fabric 1.0* and *McDATA Fabric 1.0*. Open Fabric mode is required if you are using non-McDATA switches in your fabric. McDATA Fabric mode restricts connectivity to McDATA only switches. New switches are shipped with a default of Open Fabric mode. If this fabric only contains McData switches, then change the *Interop Mode* to *MCDATA 1.0 Fabric* mode.

Restrictions:

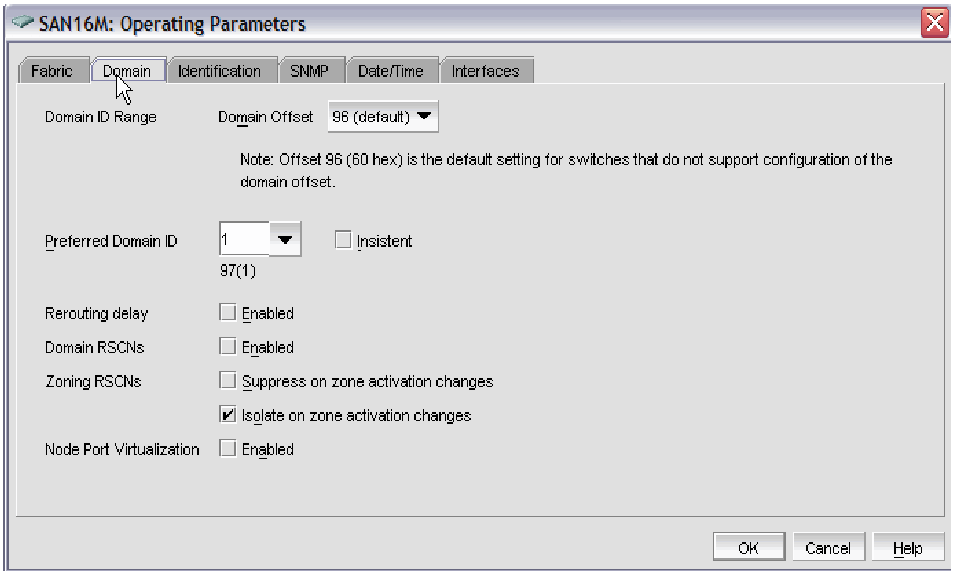
- The switch must be offline to change the Interop Mode.
- The default zone is not available in Open Fabric mode.
- Port zoning is not available in Open Fabric mode.

The R_A_TOV (resource allocation time-out value) and E_D_TOV (error detect time-out value) should be left with their default values, as they must be consistent across the entire fabric.

Switch parameters

Each switch is recognized in the fabric as a domain and is identified with a domain ID. Domains are used for the 24-bit FC addresses that identify the switch ports in a fabric. Every domain ID in the fabric must be unique ranging from 1 to 31.

To view or to change the switch parameters, we go to the Element Manager of the specific switch. Then we select **Configure** → **Operating Parameters** as shown in Figure 2-120 on page 492 and select the **Switch** tab as shown here in Figure 2-125.



Domain ID Range — Domain Offset: 96 (default)

Note: Offset 96 (60 hex) is the default setting for switches that do not support configuration of the domain offset.

Preferred Domain ID: 1 ☐ Insistent
97(1)

Rerouting delay: ☐ Enabled

Domain RSCNs: ☐ Enabled

Zoning RSCNs: ☐ Suppress on zone activation changes
☑ Isolate on zone activation changes

Node Port Virtualization: ☐ Enabled

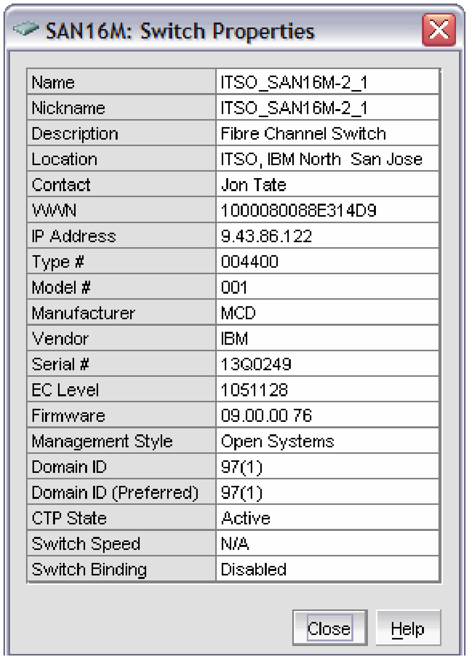
Figure 2-125 Element Manager: Configure Operating Parameters, Switch

Domain ID.... We can change the preferred domain ID and other Fibre Channel parameters for the switch.

A distinct domain ID is automatically allocated to each Switch in the fabric by the principal Switch. A fabric Switch cannot contain the same domain ID as another Switch or their E_Ports will segment when they try to join as a fabric. The Domain ID Range options allow you to configure or expand the range of possible domain IDs in a fabric from the legacy McDATA range of 96-127 IDs.

You can also configure the Domain Offset by Selecting the Domain Offset option and value from the list allows you to configure the domain offset values. Domain IDs minus the offset are still in the 1-31 range.

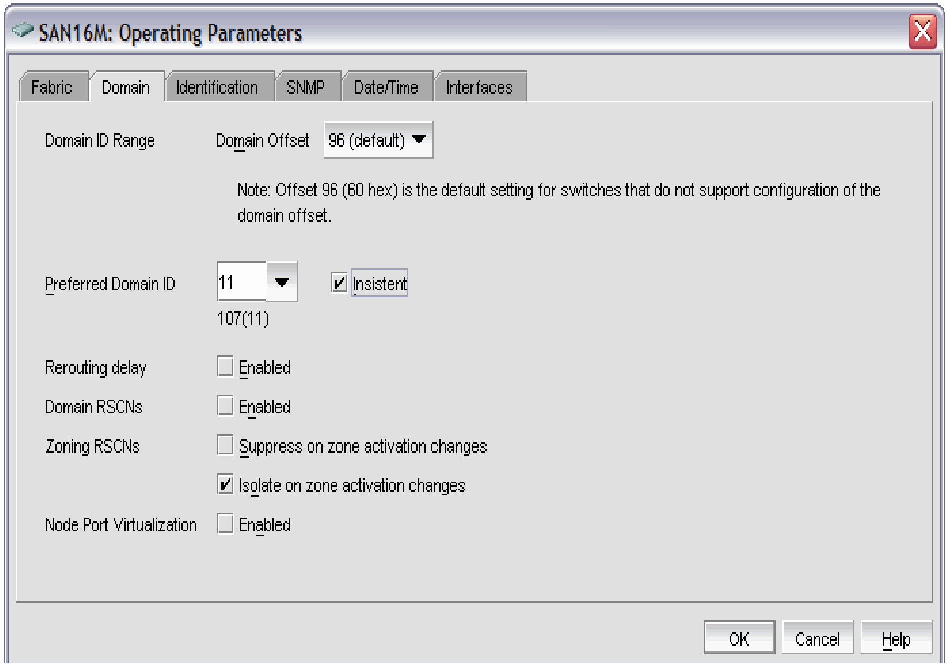
The preferred and active domain IDs can be seen in the Switch properties display, found by selecting **Product** → **Properties...** from the Element Manager, as shown in Figure 2-126.



Name	ITSO_SAN16M-2_1
Nickname	ITSO_SAN16M-2_1
Description	Fibre Channel Switch
Location	ITSO, IBM North San Jose
Contact	Jon Tate
WWN	1000080088E314D9
IP Address	9.43.86.122
Type #	004400
Model #	001
Manufacturer	MCD
Vendor	IBM
Serial #	13Q0249
EC Level	1051128
Firmware	09.00.00 76
Management Style	Open Systems
Domain ID	97(1)
Domain ID (Preferred)	97(1)
CTP State	Active
Switch Speed	N/A
Switch Binding	Disabled

Figure 2-126 Switch properties, Preferred and Active Domain IDs

We *strongly* recommend enabling the **Insistent domain** option and manually setting the domain IDs prior to building the multi-switch fabric and prior to zoning, as shown in Figure 2-127. This ensures that each switch gets the intended domain ID, and if it cannot, it will not join the fabric.



Domain ID Range Domain Offset 96 (default)

Note: Offset 96 (60 hex) is the default setting for switches that do not support configuration of the domain offset.

Preferred Domain ID 11 ☑ Insistent

107(11)

Rerouting delay ☐ Enabled

Domain RSCNs ☐ Enabled

Zoning RSCNs ☐ Suppress on zone activation changes

☑ Isolate on zone activation changes

Node Port Virtualization ☐ Enabled

Figure 2-127 Insistent domain setup

The domain ID is used to identify switch ports when port zoning is implemented. If domain IDs are negotiated at every fabric start up, there is no guarantee that the same switch will have the same ID next time, and therefore any zoning definitions might become invalid.

Restriction: The switch must be offline to change the domain ID.

Rerouting delay. This option is only applicable if the configured Switch is in a multi fabric. Enabling the rerouting delay ensures that frames are delivered in order through the fabric to their destination. If there is a change to the fabric topology that creates a new path (for example, a new Switch is added to the fabric), frames can be routed over this new path if its hop count is less than a previous path with a minimum hop count. This might result in frames being delivered to a destination out of order since frames sent over the new, shorter path might arrive ahead of older frames still in route over the older path.

If rerouting delay is enabled, traffic ceases in the fabric for the time specified in the E_D_TOV field of the Configure Fabric Parameters dialog box. This delay allows frames sent on the old path to exit to their destination before new frames begin traversing the new path.

Note: This option is disabled if Enterprise Fabric Mode (optional SANtegrity Binding feature) is enabled.

Domain RSCNs. Domain register for state change notifications (domain RSCNs) are sent between end devices in a fabric to provide additional connection information to host bus adapters (HBA) and storage devices. As an example, this information might be that a logical path has been broken because of a physical event, such as a fiber optic cable being disconnected from a port. Consult with your HBA and storage device vendor to determine if enabling Domain RSCNs will cause problems with your HBA or storage products. For example, some host bus adapters (HBAs) might log out, then log back into the fabric when they receive an RSCN, thereby disrupting Fibre Channel traffic.

Note: This option is disabled if Enterprise Fabric Mode (optional SANtegrity Binding feature) is enabled.

Zoning RSCNs. Fabric format domain RSCNs are sent to Switch ports following any change to the fabric's active zone set. These changes include activating and deactivating the zone set, or enabling and disabling the default zone. When a device receives an RSCN, this can disrupt normal activity because the device must then determine status of other devices. RSCNs can also cause some devices to write messages to error logs.

Click the check box for *Suppress on zone activation changes* or *Isolate on zone activation changes*:

- **Suppress on zone activation changes**. When this is enabled, fabric format RSCNs are not sent for zone changes to the attached devices on the Switch. This option, in most cases, should be enabled so that attached devices can receive notification of zoning changes in the fabric. However, some HBAs might log out, then log back into the fabric when they receive an RSCN, thereby disrupting Fibre Channel traffic. Consult with your HBA and storage device vendor to determine if disabling this option (and thereby enabling RSCN transmission) will cause problems with your HBA or storage products.
- **Isolate on zone activation changes.** When enabled, only devices that require RSCN notification due to a zoning configuration change receive RSCNs. Notice that this option does not have to be enabled if *Suppress on zone set activations* is enabled, since RSCNs are not sent to attached devices.

Node Port Virtualization. Node port virtualization is a method for assigning multiple Fibre Channel addresses to a single N_Port port, and is mainly used for systems that support multiple images behind a single node port.

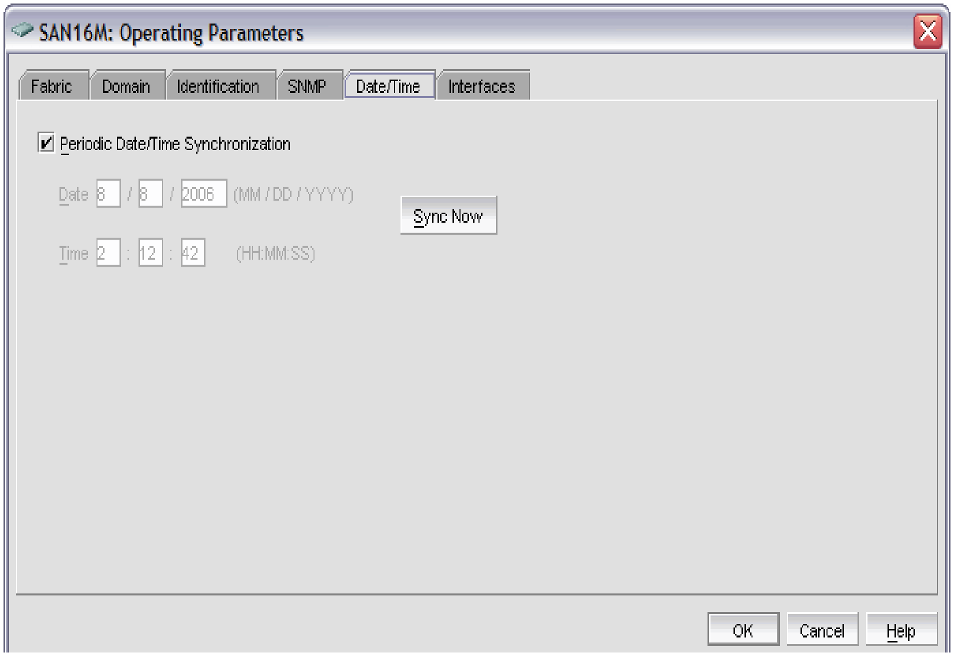
Notes:

- Node Port Virtualization does not display for a Switch that is not at the correct firmware level. If a user activates the node port virtualization feature and the Switch is at the correct firmware level, but the feature key is not installed, then an error message displays.
- If you intend to use z/Linux on an IBM System z9, you might want to enable the *NPIV* option.

Configuring switch date and time

For fabrics managed by EFCM, the switches can be configured to automatically synchronize their clocks with that of the EFCM server. This is done by launching the Element Manager and selecting use the **Configure** → **Operating Parameters** as shown in Figure 2-120 on page 492.

Select the **Date/Time** tab, and then check the **Periodic Date/Time Synchronization** box, as shown in Figure 2-128.



☑ Periodic Date/Time Synchronization

Date 8 / 8 / 2006 (MM / DD / YYYY)

Time 2 : 12 : 42 (HH:MM:SS)

Figure 2-128 Setting automatic time synchronization

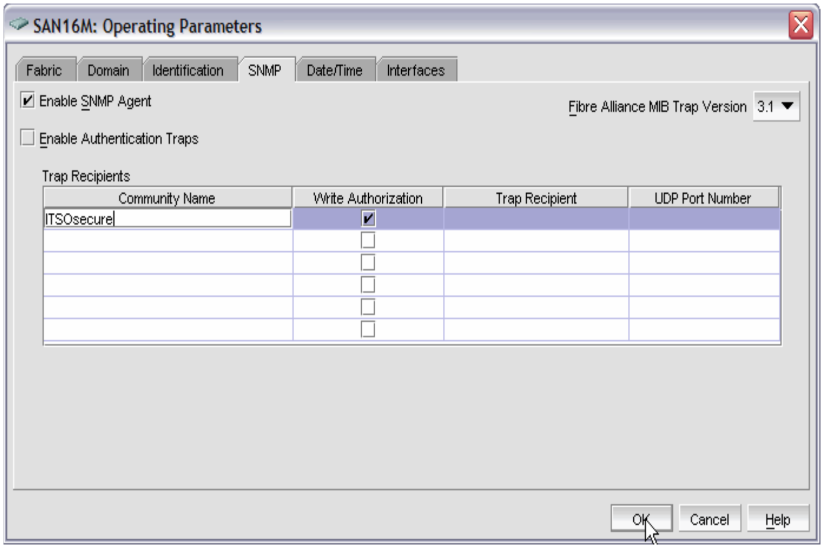
Tip: If possible, configure the operating system of the EFCM server to automatically synchronize its clock with a network time server. This helps to ensure that log records have meaningful time-stamps.

SNMP settings

Starting with E/OS 7.0, it is essential that the SNMP community string values set in each switch via Element Manager and in EFCM discovery match. During initial EFCM device discovery (see 2.14.11, “Discovering the switch with EFC Manager” on page 452) we left the community strings with their default values. For security reasons, these defaults should now be changed.

From Element Manager select **Configure** → **Operating Parameters** as shown in Figure 2-120 on page 492.

Select the **SNMP** tab, and enter a valid `community string`. Remember to check the **Enable SNMP Agent** box as shown in Figure 2-129 and click **OK**. You should now close the Element Manager window, ready to update the EFCM discovery settings.



☑ Enable SNMP Agent

Fibre Alliance MIB Trap Version 3.1

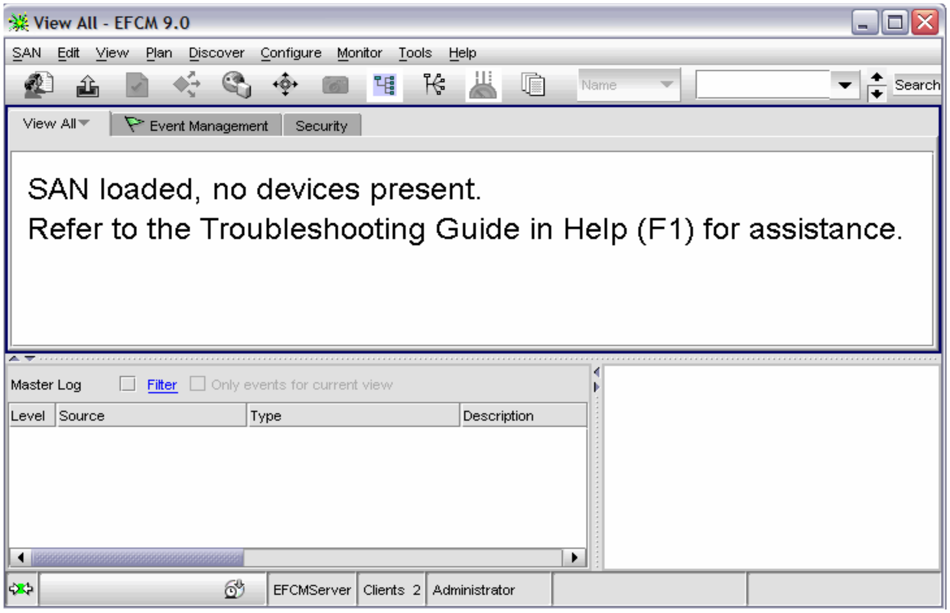
☐ Enable Authentication Traps

Trap Recipients

Community Name	Write Authorization	Trap Recipient	UDP Port Number
ITSOsecure	☑		
	☐		
	☐		
	☐		
	☐		
	☐		

Figure 2-129 SNMP configuration in Element Manager

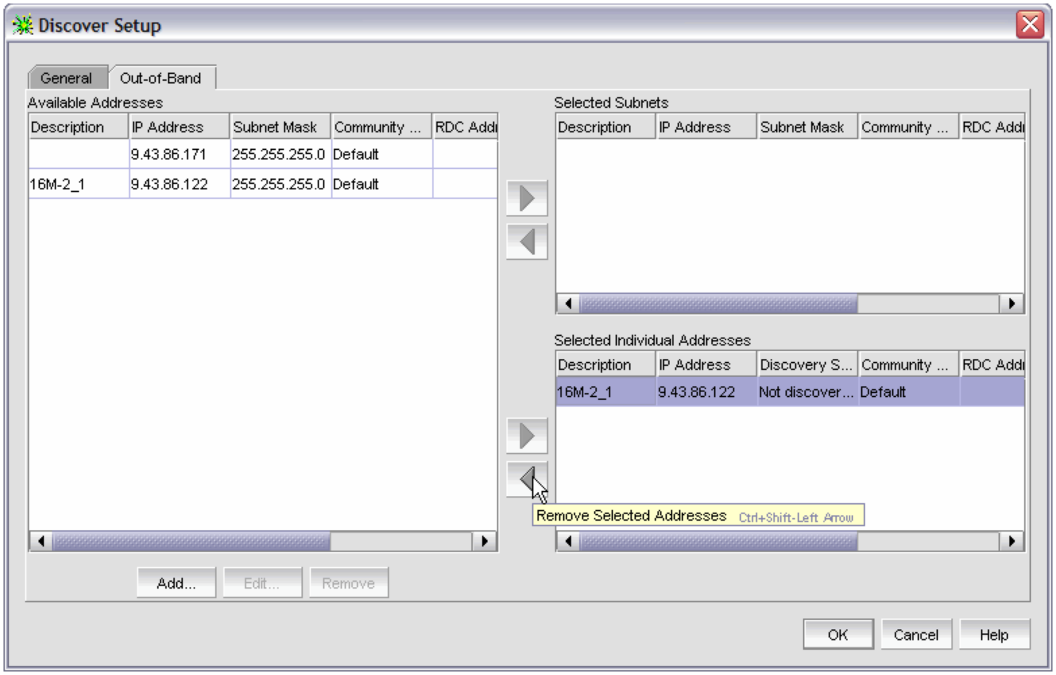
The EFCM window should now change to that shown in Figure 2-130, as it no longer has the correct community strings for the switch.


View All - EFCM 9.0
SAN Edit View Plan Discover Configure Monitor Tools Help
Name
Search
View All
Event Management
Security
Master Log
Filter
Only events for current view
Level
Source
Type
Description
EFCMServer
Clients 2
Administrator

SAN loaded, no devices present.
Refer to the Troubleshooting Guide in Help (F1) for assistance.

Figure 2-130 EFCM loss of access due to change of community strings

On the EFCM client, select **Discover** → **Setup** and a dialog box similar to that shown in Figure 2-131 should appear. In the right-hand panel, highlight the switch you have just modified and click the left arrow button to remove it. Now highlight it in the left-hand panel and click **Edit**.


Discover Setup
General
Out-of-Band
Remove Selected Addresses Ctrl+Shift-Left Arrow
Add...
Edit...
Remove
OK
Cancel
Help

Available Addresses

Description	IP Address	Subnet Mask	Community ...	RDC Add
	9.43.86.171	255.255.255.0	Default	
16M-2_1	9.43.86.122	255.255.255.0	Default	

Selected Subnets

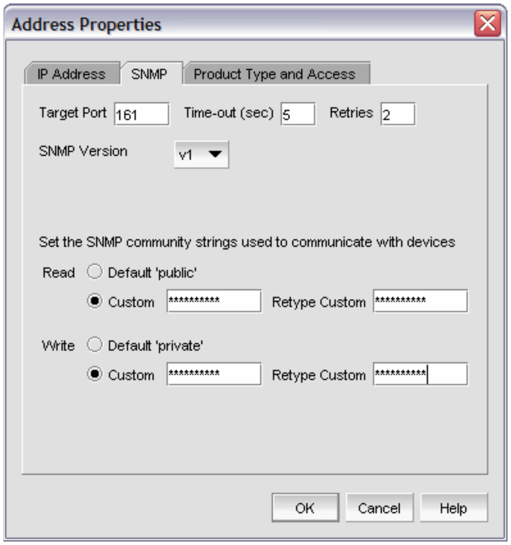
Description	IP Address	Subnet Mask	Community ...	RDC Add

Selected Individual Addresses

Description	IP Address	Discovery S...	Community ...	RDC Add
16M-2_1	9.43.86.122	Not discover...	Default	

Figure 2-131 EFCM discovery setup

Select the **SNMP** tab as shown in Figure 2-132 and change the radio buttons for Read and Write to **Custom**, and enter the same **community string** as you specified earlier in the Element Manager dialogue. Click **OK** to finish.



Target Port 161 Time-out (sec) 5 Retries 2

SNMP Version v1

Set the SNMP community strings used to communicate with devices

Read ○ Default 'public'
● Custom ********** Retype Custom **********

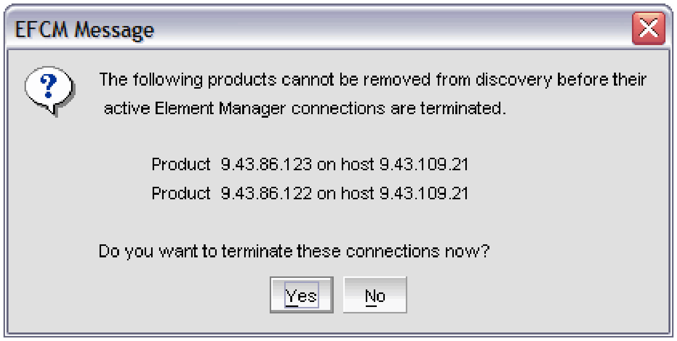
Write ○ Default 'private'
● Custom ********** Retype Custom **********

Figure 2-132 Element Manager SNMP community strings

Tip: EFCM supports the use of Ctrl-V to paste text from the clipboard.

Now click the right arrow to add the switch back to the right-hand panel and click **OK**.

Note: If you failed to close the Element Manager session after changing the switch's SNMP settings above, you see a warning similar to that in Figure 2-133.



The following products cannot be removed from discovery before their active Element Manager connections are terminated.

Product 9.43.86.123 on host 9.43.109.21
Product 9.43.86.122 on host 9.43.109.21

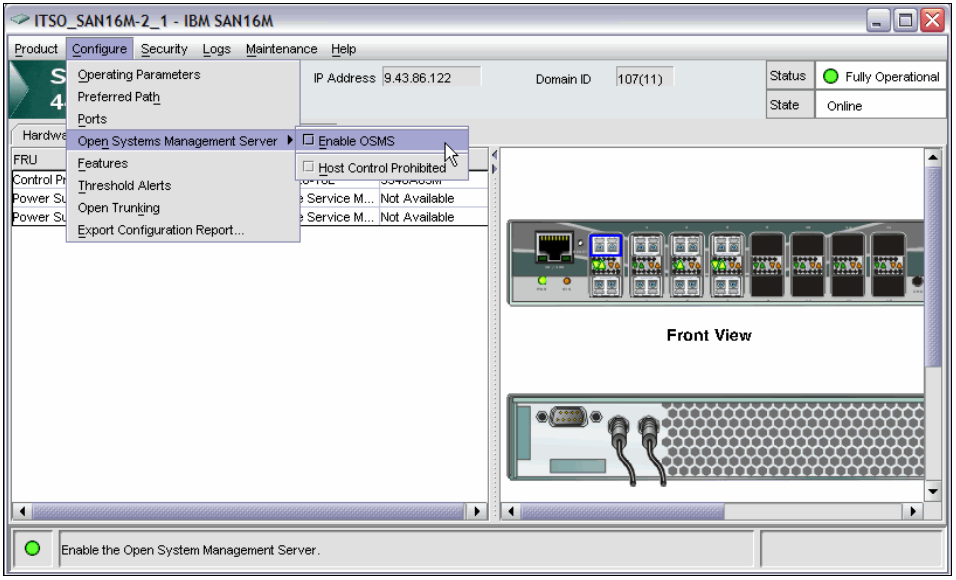
Do you want to terminate these connections now?

Figure 2-133 Active session warning

Select **Discover** and check that the **On** radio button is selected. After discovery has re-run, the switch should reappear. The discovery process might take a few minutes to run.

OSMS

If you are using open systems in-band management, then you have to ensure that this feature is enabled. From Element Manager select **Configure** → **Open Systems Management Server** and check the **Enable OSMS** check box, as shown in Figure 2-134.


ITSO_SAN16M-2_1 - IBM SAN16M
Product
Configure
Security
Logs
Maintenance
Help
Operating Parameters
Preferred Path
Ports
Open Systems Management Server
Features
Threshold Alerts
Open Trunking
Export Configuration Report...
☐ Enable OSMS
☐ Host Control Prohibited
Hardwa
FRU
Control Pr
Power Su
Power Su
Service M...
Not Available
Service M...
Not Available
Front View

IP Address 9.43.86.122

Domain ID 107(11)

Status ● Fully Operational

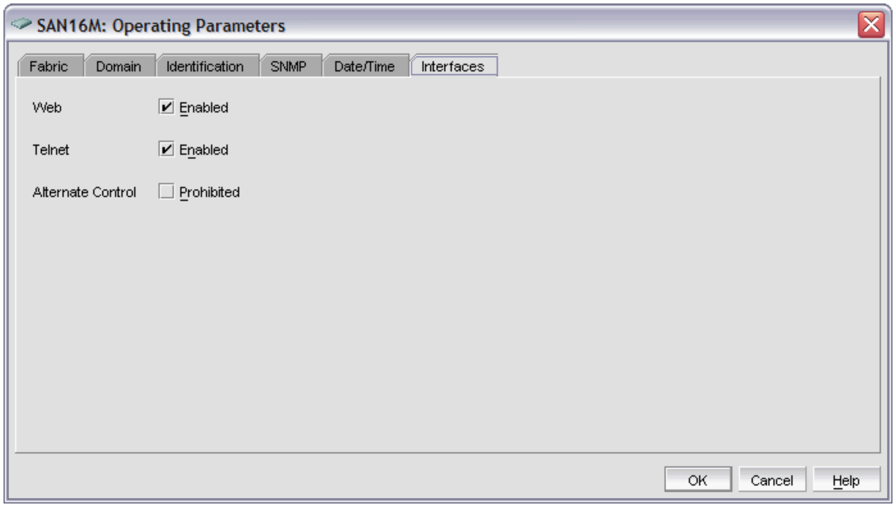
State Online

Enable the Open System Management Server.

Figure 2-134 Enable OSMS

Telnet and Web server access

By default, both Telnet CLI access and Web server access is enabled. If you have the requirement to disable either one, this is done From Element Manager. Select **Configure** → **Operating Parameters** as shown in Figure 2-120 on page 492. Click the **Interfaces** tab and you can enable and disable Telnet and the Web server from this window, as shown here in Figure 2-135.


SAN16M: Operating Parameters
Fabric
Domain
Identification
SNMP
Date/Time
Interfaces
OK
Cancel
Help

Web ☑ Enabled

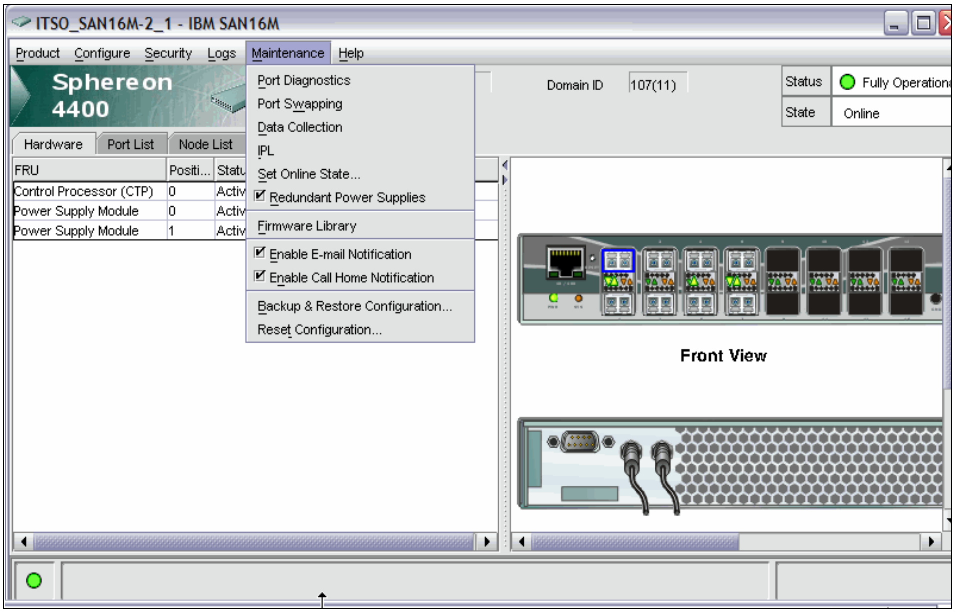
Telnet ☑ Enabled

Alternate Control ☐ Prohibited

Figure 2-135 Telnet and Web server access

E-mail alerts

To ensure that e-mail alerts will be sent, click the **Maintenance** pull-down menu and confirm that the **Enable E-Mail Notification** check box is checked, as shown in Figure 2-136.


ITSO_SAN16M-2_1 - IBM SAN16M
Product
Configure
Security
Logs
Maintenance
Help
Sphereon 4400
Hardware
Port List
Node List
Port Diagnostics
Port Swapping
Data Collection
IPL
Set Online State...
Firmware Library
Backup & Restore Configuration...
Reset Configuration...
Front View

☑ Redundant Power Supplies

☑ Enable E-mail Notification

☑ Enable Call Home Notification

Domain ID 107(11)

Status ● Fully Operationa

State Online

FRU	Positi...	Statu
Control Processor (CTP)	0	Activ
Power Supply Module	0	Activ
Power Supply Module	1	Activ

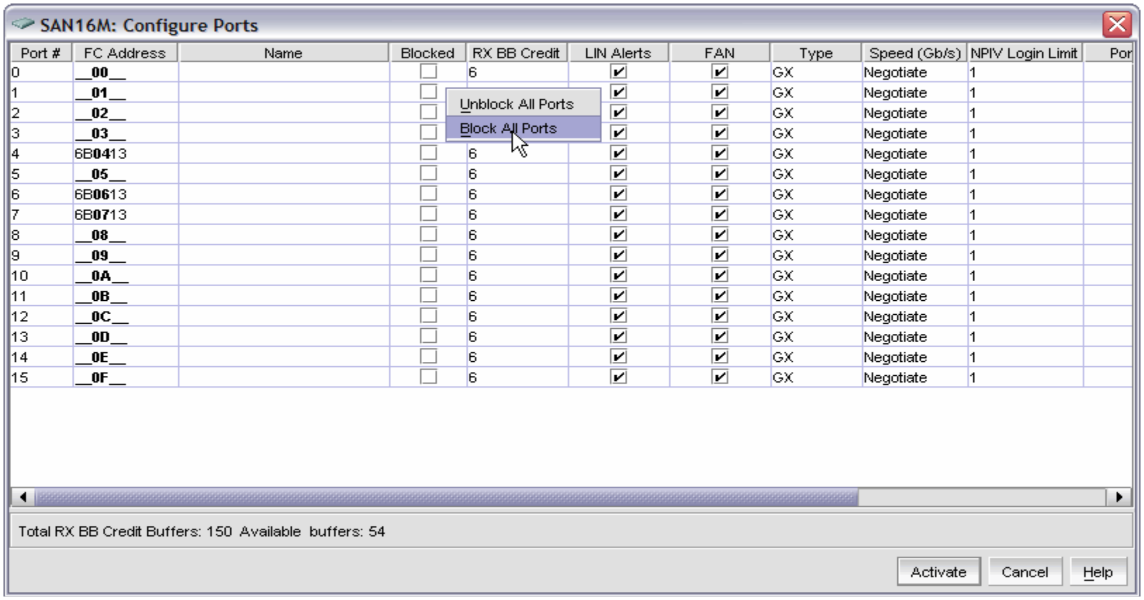
Figure 2-136 Checking E-Mail and Call Home are enabled

Call Home

To ensure that call home will occur, click the **Maintenance** pull-down menu and confirm that the **Call-Home Notification** check box is checked, as shown in Figure 2-136 on page 507.

Port configuration

It is wise to keep unused ports blocked, as this helps control device connectivity, so from Element Manager select **Configure** → **Ports...** and in the panel that displays, right-click in the **Blocked** column and select **Block All Ports**, as shown in Figure 2-137. Then click **Activate**.



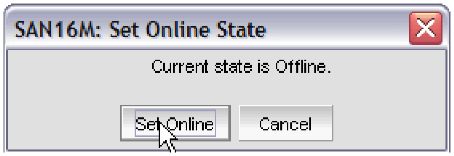
Port #	FC Address	Name	Blocked	RX BB Credit	LIN Alerts	FAN	Type	Speed (Gb/s)	NPIV Login Limit	Por
0	__00__		☐	6	☑	☑	GX	Negotiate	1	
1	__01__		☐		☑	☑	GX	Negotiate	1	
2	__02__		☐		☑	☑	GX	Negotiate	1	
3	__03__		☐		☑	☑	GX	Negotiate	1	
4	6B0413		☐	6	☑	☑	GX	Negotiate	1	
5	__05__		☐	6	☑	☑	GX	Negotiate	1	
6	6B0613		☐	6	☑	☑	GX	Negotiate	1	
7	6B0713		☐	6	☑	☑	GX	Negotiate	1	
8	__08__		☐	6	☑	☑	GX	Negotiate	1	
9	__09__		☐	6	☑	☑	GX	Negotiate	1	
10	__0A__		☐	6	☑	☑	GX	Negotiate	1	
11	__0B__		☐	6	☑	☑	GX	Negotiate	1	
12	__0C__		☐	6	☑	☑	GX	Negotiate	1	
13	__0D__		☐	6	☑	☑	GX	Negotiate	1	
14	__0E__		☐	6	☑	☑	GX	Negotiate	1	
15	__0F__		☐	6	☑	☑	GX	Negotiate	1	

Total RX BB Credit Buffers: 150 Available buffers: 54

Figure 2-137 Initial port blocking

Verify switch is online

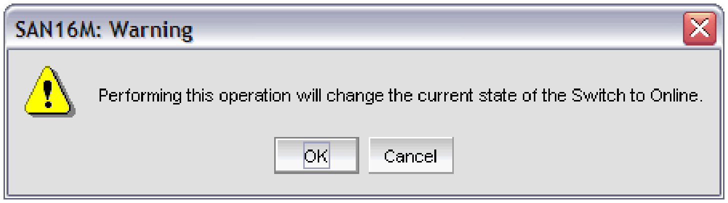
Lastly, remember to check that the switch is online, or no FC traffic can flow. Select **Maintenance** → **Set Online State...** and confirm that the current state is ONLINE, as shown in Figure 2-138. If it is not, click **Set Online**.



Current state is Offline.

Figure 2-138 Current state is online

You then get the message shown in Figure 2-139. Click the **OK** button to bring the switch online.



Performing this operation will change the current state of the Switch to Online.

Figure 2-139 Online warning window

2.14.16 Connecting fiber optics to switch ports

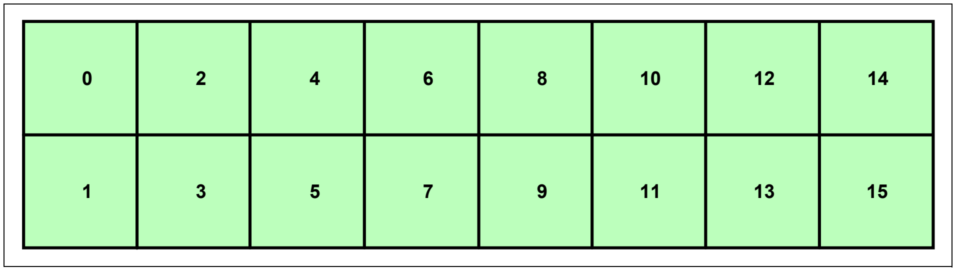
This section covers items to remember when connecting new host or storage ports to switch or director ports.

Physical port layout

We show the port layouts of various switches in the topics that follow.

SAN16M-2 port layout

The SAN16M-2 is a half-width switch with ports on the front numbered as shown in Figure 2-140. It is based on the Atlas ASIC, and provides a shared buffer pool for each set of four ports (0-3, 4-7, 8-11 and 12-15). As such, connections requiring a greater number of BB Credits should be distributed evenly across the ASICs.

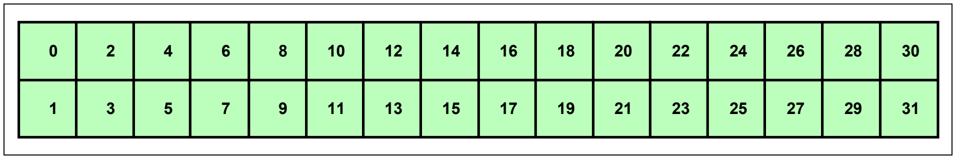


0	2	4	6	8	10	12	14
1	3	5	7	9	11	13	15

Figure 2-140 SAN16M-2 ports (front)

SAN32M-2 port layout

The SAN32M-2 is a full-width switch with ports on the front numbered as shown in Figure 2-141. It is based on the Pegasus ASIC, and provides a shared buffer pool for each set of four ports (0-3, 4-7, 8-11 ... 28-31). As with the SAN16M-2, connections requiring a greater number of BB Credits should be distributed evenly across the ASICs.



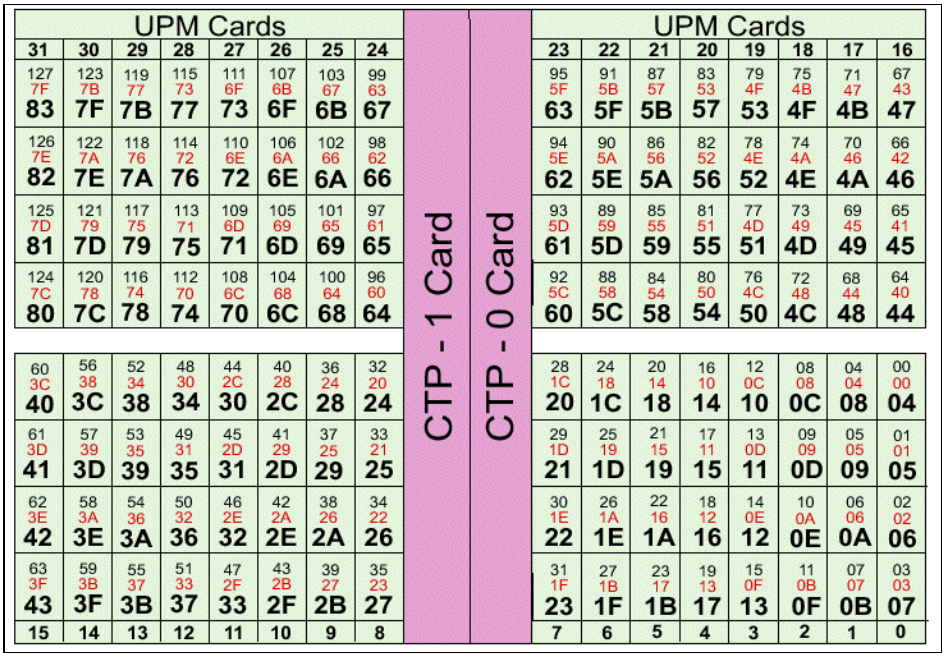
0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31

Figure 2-141 SAN32M-2 port layout (front)

SAN140M port layout

The director contains ports at the front and the rear of the director. The ports on the front are numbered from 0-127 and continue on the rear from 132-143. Ports 128-131 are not available ports.

In Figure 2-142 we show the numbering scheme for the front ports. On the bottom, the port count starts at the right-most UPM and goes from the top to the bottom on each UPM. On the top, the port count continues from the right-most UPM but the count now starts from the bottom to the top of each UPM; this is because the cards on the top are physically installed upside-down compared to the bottom cards.

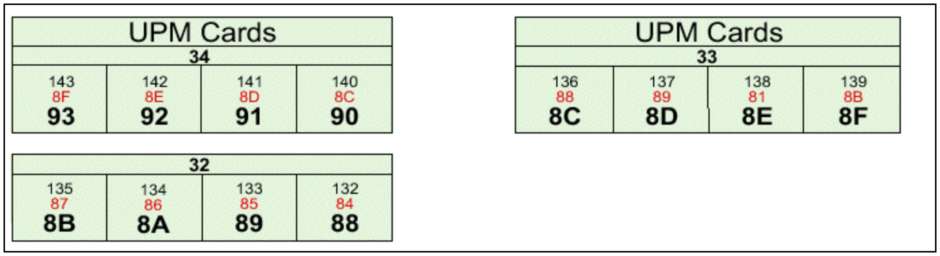


UPM Cards										UPM Cards							
31	30	29	28	27	26	25	24	CTP - 1 Card	CTP - 0 Card	23	22	21	20	19	18	17	16
127 7F 83	123 7B 7F	119 77 7B	115 73 77	111 6F 73	107 6B 6F	103 67 6B	99 63 67			95 5F 63	91 5B 5F	87 57 5B	83 53 57	79 4F 53	75 4B 4F	71 47 4B	67 43 47
126 7E 82	122 7A 7E	118 76 7A	114 72 76	110 6E 72	106 6A 6E	102 66 6A	98 62 66			94 5E 62	90 5A 5E	86 56 5A	82 52 56	78 4E 52	74 4A 4E	70 46 4A	66 42 46
125 7D 81	121 79 7D	117 75 79	113 71 75	109 6D 71	105 69 6D	101 65 69	97 61 65			93 5D 61	89 59 5D	85 55 59	81 51 55	77 4D 51	73 49 4D	69 45 49	65 41 45
124 7C 80	120 78 7C	116 74 78	112 70 74	108 6C 70	104 68 6C	100 64 68	96 60 64			92 5C 60	88 58 5C	84 54 58	80 50 54	76 4C 50	72 48 4C	68 44 48	64 40 44
60 3C 40	56 38 3C	52 34 38	48 30 34	44 2C 30	40 28 2C	36 24 28	32 20 24			28 1C 20	24 18 1C	20 14 18	16 10 14	12 0C 10	08 08 0C	04 04 08	00 00 04
61 3D 41	57 39 3D	53 35 39	49 31 35	45 2D 31	41 29 2D	37 25 29	33 21 25			29 1D 21	25 19 1D	21 15 19	17 11 15	13 0D 11	09 09 0D	05 05 09	01 01 05
62 3E 42	58 3A 3E	54 36 3A	50 32 36	46 2E 32	42 2A 2E	38 26 2A	34 22 26			30 1E 22	26 1A 1E	22 16 1A	18 12 16	14 0E 12	10 0A 0E	06 06 0A	02 02 06
63 3F 43	59 3B 3F	55 37 3B	51 33 37	47 2F 33	43 2B 2F	39 27 2B	35 23 27			31 1F 23	27 1B 1F	23 17 1B	19 13 17	15 0F 13	11 0B 0F	07 07 0B	03 03 07
15	14	13	12	11	10	9	8			7	6	5	4	3	2	1	0

Figure 2-142 SAN140M port map (front)

Note: The large, bold, hexadecimal numbers are the Link Port Addresses used for FICON IOCP configurations on zSeries processors. For FCP traffic, the top decimal number of the three numbers shown in each port is the port number used.

In Figure 2-143 we show the numbering scheme for the rear ports. This scheme is slightly different. On the bottom left UPM, the ports count from right to left; the next sequential UPM is on the top right card, where the ports count from left to right; and finally, the top left card, where the ports count from right to left.



UPM Cards

34			
143 8F **93**	142 8E **92**	141 8D **91**	140 8C **90**

32			
135 87 **8B**	134 86 **8A**	133 85 **89**	132 84 **88**

UPM Cards

33			
136 88 **8C**	137 89 **8D**	138 81 **8E**	139 8B **8F**

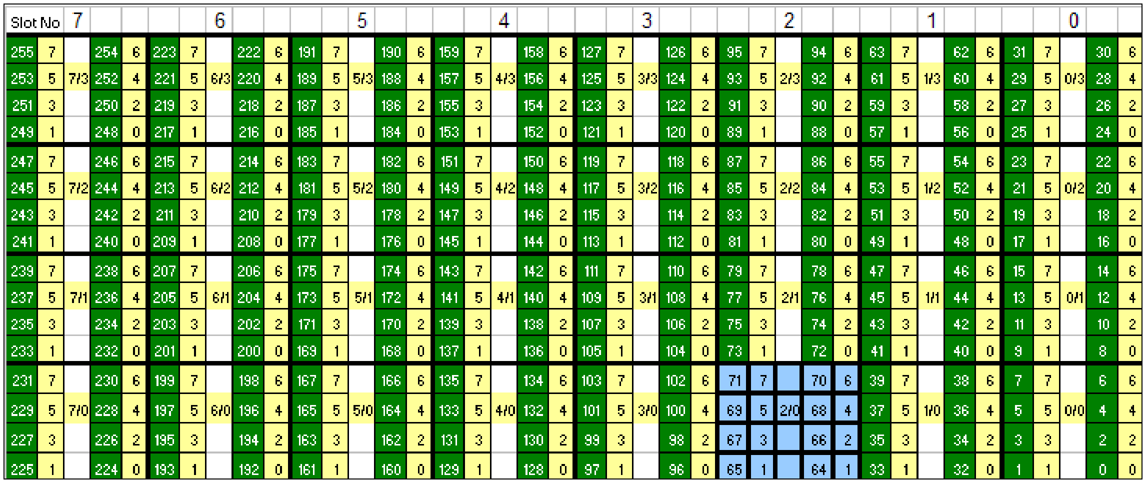
Figure 2-143 SAN140M port map (rear)

For availability purposes on directors, we recommend that you spread your storage ports across multiple cards. Servers with multiple HBAs connected to the director should also be connected to ports spread across multiple cards, as should any ISLs to another director or switch. In the event of a UPM card failure, only a single link to a given storage device or server is impacted, which minimizes any performance degradation.

SAN256M port layout

The ports are numbered in the range 0 to 255, from right to left and bottom to top. The port number is the same as the port address.

Due to the use of Line Modules (LIMs) and Optical Paddles, each port also has a port locator number which identifies its physical location, in the format x/y/z, as illustrated in Figure 2-144. For eight-port paddles, the ports are numbered 0-7 within the paddle, while for two-port paddles the ports are numbered 0 and 4.



Slot No		7					6					5					4					3					2					1					0		
255	7		254	6	223	7		222	6	191	7		190	6	159	7		158	6	127	7		126	6	95	7		94	6	63	7		62	6	31	7		30	6
253	5	7/3	252	4	221	5	6/3	220	4	189	5	5/3	188	4	157	5	4/3	156	4	125	5	3/3	124	4	93	5	2/3	92	4	61	5	1/3	60	4	29	5	0/3	28	4
251	3		250	2	219	3		218	2	187	3		186	2	155	3		154	2	123	3		122	2	91	3		90	2	59	3		58	2	27	3		26	2
249	1		248	0	217	1		216	0	185	1		184	0	153	1		152	0	121	1		120	0	89	1		88	0	57	1		56	0	25	1		24	0
247	7		246	6	215	7		214	6	183	7		182	6	151	7		150	6	119	7		118	6	87	7		86	6	55	7		54	6	23	7		22	6
245	5	7/2	244	4	213	5	6/2	212	4	181	5	5/2	180	4	149	5	4/2	148	4	117	5	3/2	116	4	85	5	2/2	84	4	53	5	1/2	52	4	21	5	0/2	20	4
243	3		242	2	211	3		210	2	179	3		178	2	147	3		146	2	115	3		114	2	83	3		82	2	51	3		50	2	19	3		18	2
241	1		240	0	209	1		208	0	177	1		176	0	145	1		144	0	113	1		112	0	81	1		80	0	49	1		48	0	17	1		16	0
239	7		238	6	207	7		206	6	175	7		174	6	143	7		142	6	111	7		110	6	79	7		78	6	47	7		46	6	15	7		14	6
237	5	7/1	236	4	205	5	6/1	204	4	173	5	5/1	172	4	141	5	4/1	140	4	109	5	3/1	108	4	77	5	2/1	76	4	45	5	1/1	44	4	13	5	0/1	12	4
235	3		234	2	203	3		202	2	171	3		170	2	139	3		138	2	107	3		106	2	75	3		74	2	43	3		42	2	11	3		10	2
233	1		232	0	201	1		200	0	169	1		168	0	137	1		136	0	105	1		104	0	73	1		72	0	41	1		40	0	9	1		8	0
231	7		230	6	199	7		198	6	167	7		166	6	135	7		134	6	103	7		102	6	71	7		70	6	39	7		38	6	7	7		6	6
229	5	7/0	228	4	197	5	6/0	196	4	165	5	5/0	164	4	133	5	4/0	132	4	101	5	3/0	100	4	69	5	2/0	68	4	37	5	1/0	36	4	5	5	0/0	4	4
227	3		226	2	195	3		194	2	163	3		162	2	131	3		130	2	99	3		98	2	67	3		66	2	35	3		34	2	3	3		2	2
225	1		224	0	193	1		192	0	161	1		160	0	129	1		128	0	97	1		96	0	65	1		64	1	33	1		32	0	1	1		0	0

Figure 2-144 SAN256M port layout and port locators (front), 1,2,4 GBps ports

A port number can be calculated from the port locator number as:

```
(LIM_number x 32) + (paddle_number x 8) + paddle_port = port_number
```

So the top left port in the blue eight-port paddle 0 in LIM 2 is:

```
(2 x 32) + (0 x 8) + 7 = 71
```

Figure 2-145 shows the port numbering for a SAN256M director with 10Gbps LIM's installed. So for example the 10Gbps port shown as n+20 is as follows, Assuming this is plugged into slot 2.

The rule is the same:

```
(LIM_number x 32) + (paddle_number x 8) + paddle_port = port_number
```

```
(2 x 32) + (2 x 8) + 4 = 84
```

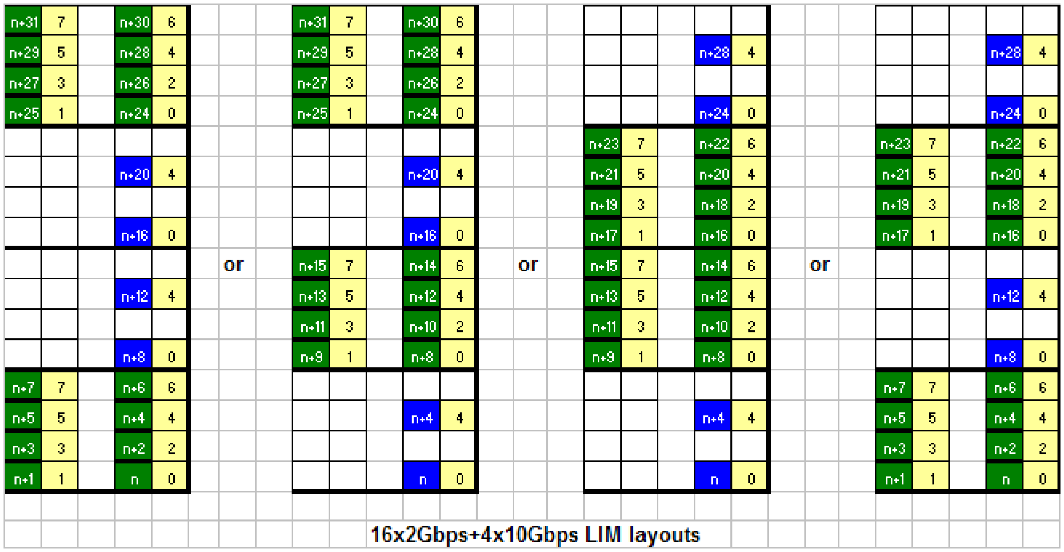


Figure 2-145   SAN256B port numbering 10Gbs ports

Fiber optic cable labelling

It is a best practice to attach labels to all cables used in a SAN and to maintain a record of all connections made, either with a spreadsheet or a dedicated cabling database. It is best to use a simple numbering scheme for the label, rather than try to encode information about what it connects to, and use your cabling records to detail such information as where the cable goes and what it is connected to.

There are two styles of label commonly used with cables, namely *flag* and *wrap*. Figure 2-146 shows examples of the flag style on the left and the wrap style on the right. Flag labels have the text printed twice, and are attached with equal lengths of label either side of the cable so that the label sticks to itself. Wrap labels have the text printed repeatedly across the width of the label, and are then wrapped around the cable.

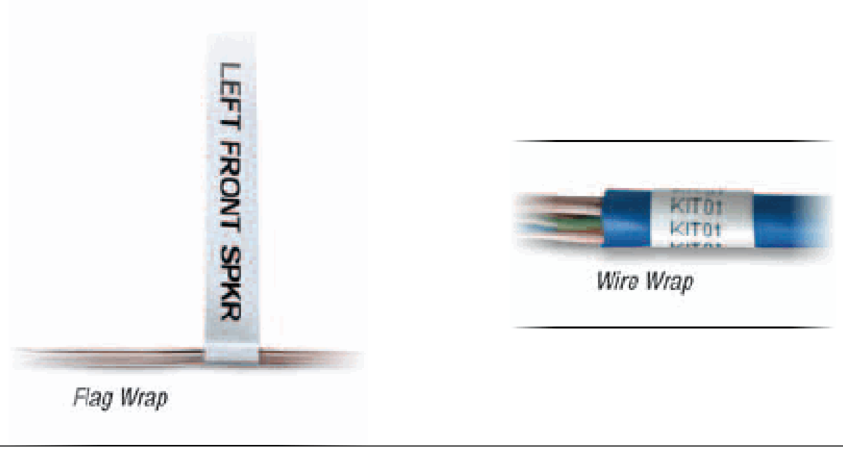


Figure 2-146 Examples of flag and wrap style labels

Tip: Wrap labels are generally easier to read than flag labels, and consume less space.

Several manufacturers produce hand-held or desktop labelling machines at reasonable prices which are capable of printing suitable labels. These usually include features which enable multiple copies and label sequences to be printed automatically.

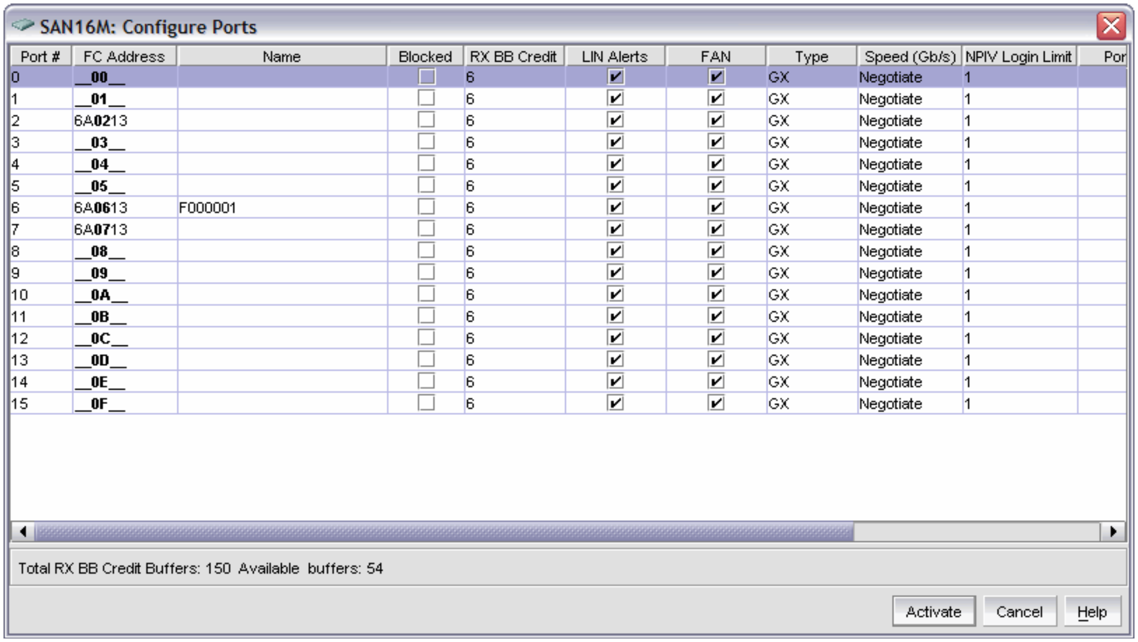
Important: Remember to attach the same label to both ends of the cable.

Port labelling

EFCM provides the ability to enter a port name against each switch or director port using the **Configure Ports** window. This is a static label assigned to the physical port, and is not related to any nicknames that might be assigned to WWNs of attached N_Ports.

A local convention should be developed which details the format of information which should be placed in the port name field. This might repeat some of the details from the cabling database, or simply contain the label of the fibre attached to that port, or possibly even be left blank. If used, it is important that the data in this field be kept current to avoid confusion.

To configure the port name relating to each port, select **Configure** → **Ports...**. and you are presented with the Configure Ports window shown in Figure 2-147. Click in the **Name** column against the port you want to name and type in the name. Now might also be a good time to unblock the port by removing the check in the **Blocked** column. Click **Activate** to finish.



Port #	FC Address	Name	Blocked	RX BB Credit	LIN Alerts	FAN	Type	Speed (Gb/s)	NPIV Login Limit	Por
0	__00__		☐	6	☑	☑	GX	Negotiate	1	
1	__01__		☐	6	☑	☑	GX	Negotiate	1	
2	6A0213		☐	6	☑	☑	GX	Negotiate	1	
3	__03__		☐	6	☑	☑	GX	Negotiate	1	
4	__04__		☐	6	☑	☑	GX	Negotiate	1	
5	__05__		☐	6	☑	☑	GX	Negotiate	1	
6	6A0613	F000001	☐	6	☑	☑	GX	Negotiate	1	
7	6A0713		☐	6	☑	☑	GX	Negotiate	1	
8	__08__		☐	6	☑	☑	GX	Negotiate	1	
9	__09__		☐	6	☑	☑	GX	Negotiate	1	
10	__0A__		☐	6	☑	☑	GX	Negotiate	1	
11	__0B__		☐	6	☑	☑	GX	Negotiate	1	
12	__0C__		☐	6	☑	☑	GX	Negotiate	1	
13	__0D__		☐	6	☑	☑	GX	Negotiate	1	
14	__0E__		☐	6	☑	☑	GX	Negotiate	1	
15	__0F__		☐	6	☑	☑	GX	Negotiate	1	

Total RX BB Credit Buffers: 150 Available buffers: 54

Figure 2-147 Element Manager - Configure port names

In this example, a fiber optic labelled `F00001` is connected to the port. The port name appears in the Element Manager to identify the port, for example in the Port Properties dialog box.

Assigning nicknames in EFCM

As with IP addresses and the DNS, managing the SAN can be made easier by defining nicknames for WWNs. This helps later when we have to identify devices, for instance, while configuring zoning.

The name can be the DNS host name in the case of only one adapter in one host. If there is more than one adapter in one host, we recommend that the nickname should consist of the hostname and some extension to distinguish between adapters. The extension could be the number from the cable’s label, or it could be related to the location of the HBA (such as its PCI slot address) within the host. Particular care should be taken with partitioned hosts such as pSeries®, where HBAs can be dedicated to partitions. For storage arrays such as the IBM TotalStorage Enterprise Storage Server Model 800, it could relate to the cluster and host bay containing the storage port, which would help ensure that storage ports are correctly zoned for maximum availability.

There are several places where nicknames can be assigned to a WWN. One is on the main window of the EFCM. Expand the list on the left to display the switches then again to display the nodes. Next, right-click a WWN and select **Properties** as shown in Figure 2-148.

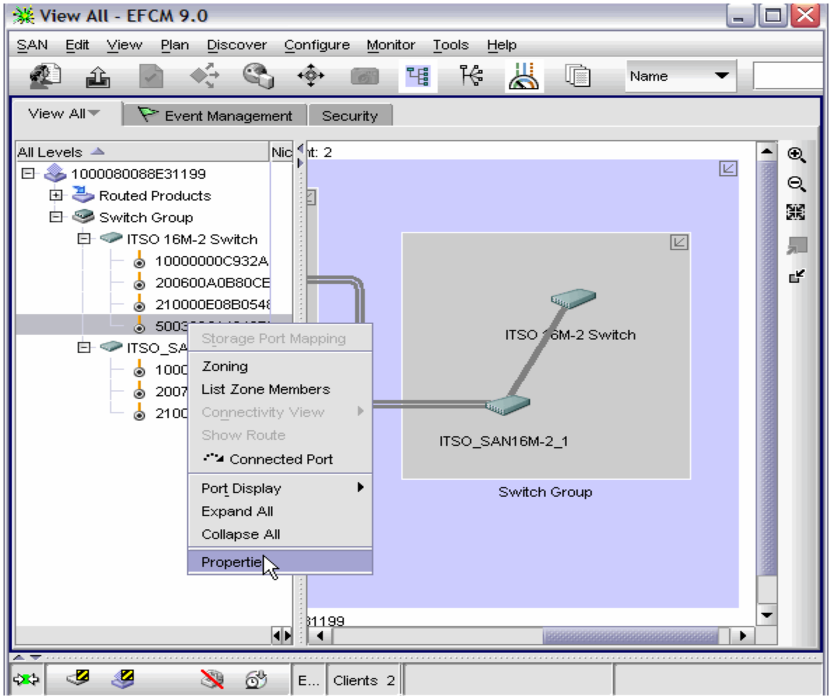
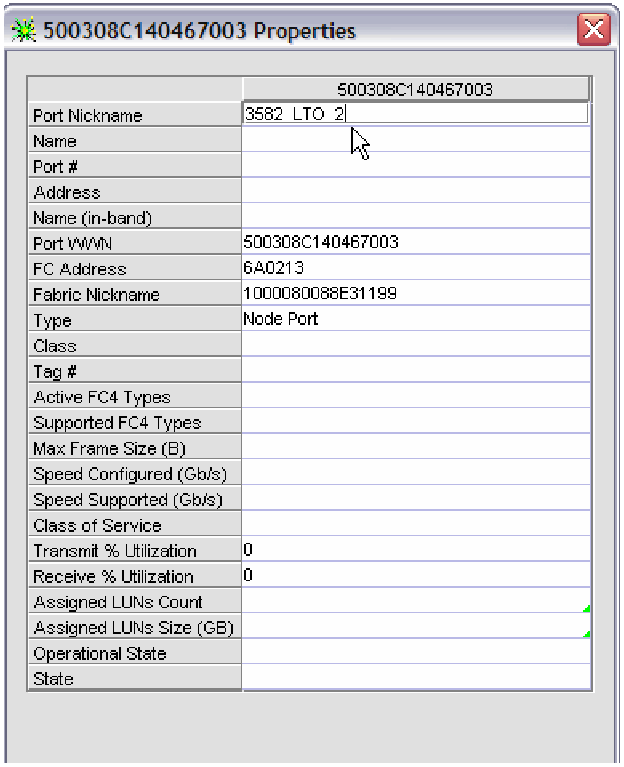

View All - EFCM 9.0
SAN Edit View Plan Discover Configure Monitor Tools Help
Name
View All
Event Management
Security
All Levels
Nic
1000080088E31199
Routed Products
Switch Group
ITSO 16M-2 Switch
10000000C932A
200600A0B80CE
210000E08B054
ITSO_SA
1000
2007
2100
Storage Port Mapping
Zoning
List Zone Members
Connectivity View
Show Route
Connected Port
Port Display
Expand All
Collapse All
Properties
ITSO 16M-2 Switch
ITSO_SAN16M-2_1
Switch Group
E...
Clients 2

Figure 2-148 EFC Manager, port name Properties

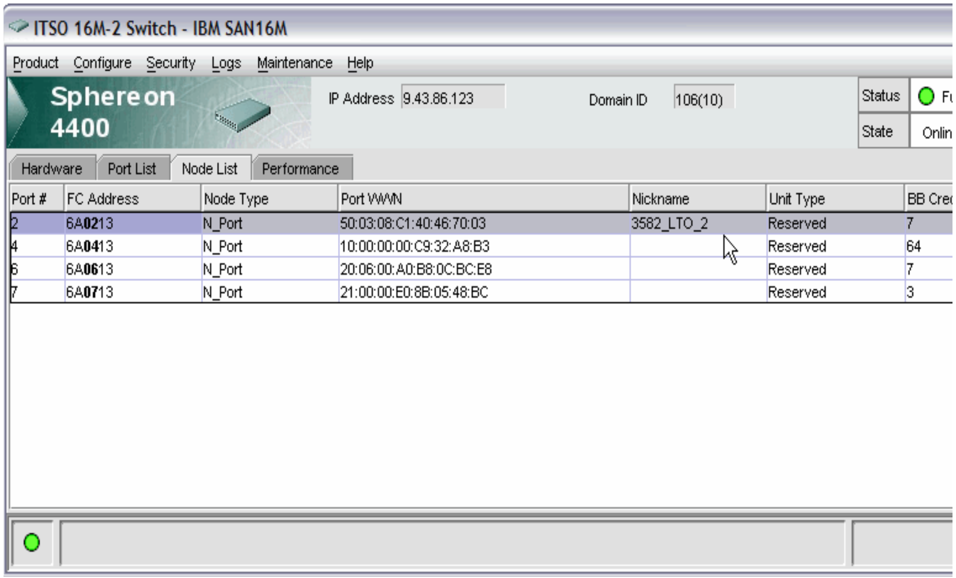
This brings up a dialog box where we enter the nickname for that device as shown in Figure 2-149.



	500308C140467003
Port Nickname	3582 LTO 2
Name	
Port #	
Address	
Name (in-band)	
Port WWN	500308C140467003
FC Address	6A0213
Fabric Nickname	1000080088E31199
Type	Node Port
Class	
Tag #	
Active FC4 Types	
Supported FC4 Types	
Max Frame Size (B)	
Speed Configured (Gb/s)	
Speed Supported (Gb/s)	
Class of Service	
Transmit % Utilization	0
Receive % Utilization	0
Assigned LUNs Count	
Assigned LUNs Size (GB)	
Operational State	
State	

Figure 2-149 EFC Manager, port Properties, assigning a nickname

A second method of assigning nicknames is from the Element Manager. Choose the **Node List** tab and right-click the port you want to assign a nickname to. Select **Define Nickname...** from the pop-up menu, as shown in Figure 2-150, and enter the nickname as shown in Figure 2-151.


ITSO 16M-2 Switch - IBM SAN16M
Product
Configure
Security
Logs
Maintenance
Help
Sphereon 4400
Status
State
Hardware
Port List
Node List
Performance

IP Address 9.43.86.123

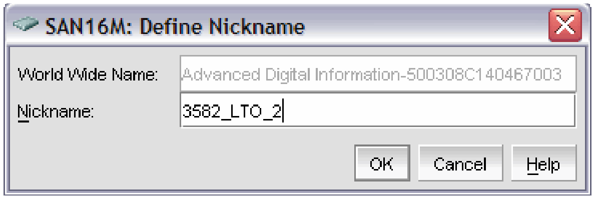
Domain ID 106(10)

Status: Fu

State: Onlin

Port #	FC Address	Node Type	Port WWN	Nickname	Unit Type	BB Cre
2	6A0213	N_Port	50:03:08:C1:40:46:70:03	3582_LTO_2	Reserved	7
4	6A0413	N_Port	10:00:00:00:C9:32:A8:B3		Reserved	64
6	6A0613	N_Port	20:06:00:A0:B8:0C:BC:E8		Reserved	7
7	6A0713	N_Port	21:00:00:E0:8B:05:48:BC		Reserved	3

Figure 2-150 Element Manager, Define Nickname

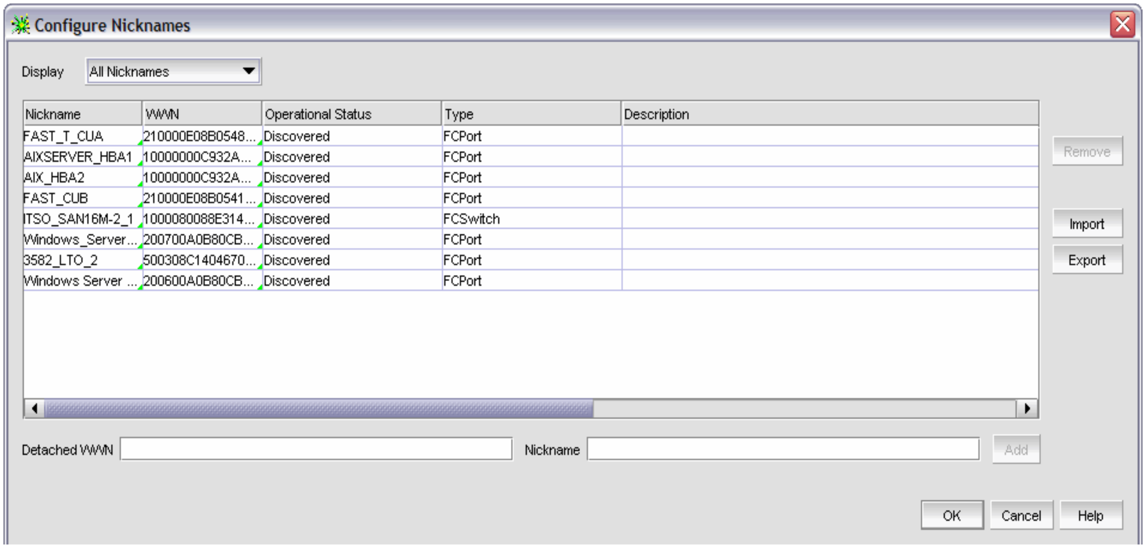

SAN16M: Define Nickname
OK
Cancel
Help

World Wide Name: Advanced Digital Information-500308C140467003

Nickname: 3582_LTO_2

Figure 2-151 Entering nickname

The EFCM also provides a nickname management facility accessed by selecting **Configure** → **Nicknames**. This allows for the addition, deletion, and updating of nicknames, and is shown in Figure 2-152. It is also possible to export or import nicknames as text files from here.



Nickname	WWN	Operational Status	Type	Description
FAST_T_CUA	210000E08B0548...	Discovered	FCPort	
AIXSERVER_HBA1	10000000C932A...	Discovered	FCPort	
AIX_HBA2	10000000C932A...	Discovered	FCPort	
FAST_CUB	210000E08B0541...	Discovered	FCPort	
ITSO_SAN16M-2_1	1000080088E314...	Discovered	FCSwitch	
Windows_Server...	200700A0B80CB...	Discovered	FCPort	
3582_LTO_2	500308C1404670...	Discovered	FCPort	
Windows Server ...	200600A0B80CB...	Discovered	FCPort	

Figure 2-152 EFCM configure nicknames

If an HBA is swapped, the nickname remains associated with the old card's WWN, and hence cannot be assigned to the replacement card's WWN. To resolve this, use the Configure Nicknames panel to delete the old nickname and then nickname the new HBA as normal. This panel can also be used to delete nicknames for old hosts that have been removed from the fabric.

Viewing by nickname

Having assigned nicknames to the attached WWNs, you might want to update the view preferences on the EFCM to display them. Change the value of the drop-down list shown in Figure 2-153 to `Nickname` to cause the EFCM to display nicknames in place of WWNs.

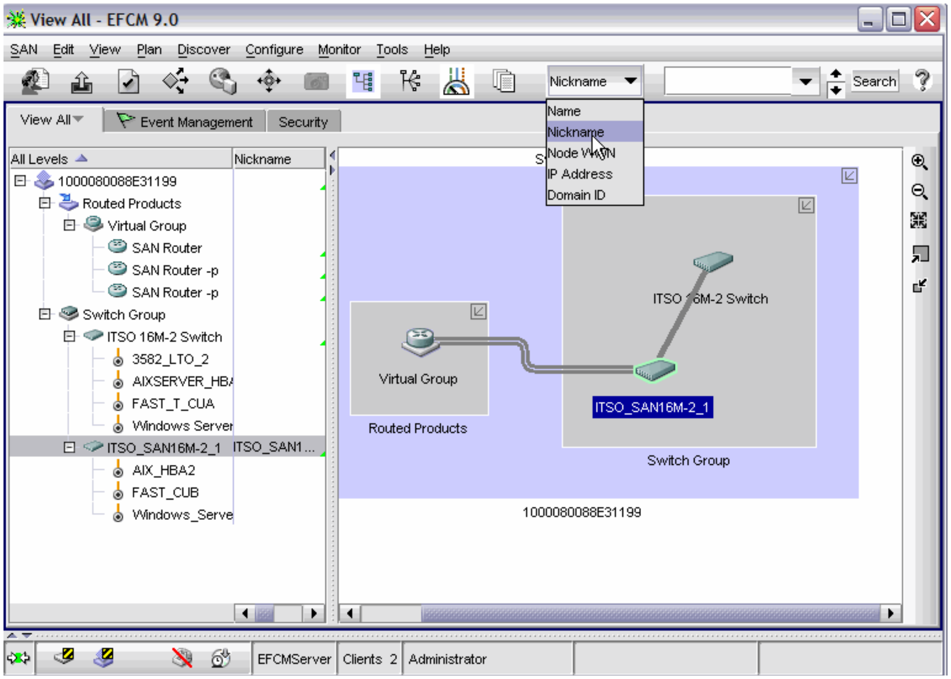

View All - EFCM 9.0
SAN Edit View Plan Discover Configure Monitor Tools Help
Nickname
Search
Name
Nickname
Node WWN
IP Address
Domain ID
View All
Event Management
Security
All Levels
Nickname
1000080088E31199
Routed Products
Virtual Group
SAN Router
SAN Router -p
SAN Router -p
Switch Group
ITSO 16M-2 Switch
3582_LTO_2
AIXSERVER_HB
FAST_T_CUA
Windows Server
ITSO_SAN16M-2_1
ITSO_SAN1...
AIX_HBA2
FAST_CUB
Windows_Serve
ITSO 16M-2 Switch
Virtual Group
ITSO_SAN16M-2_1
Routed Products
Switch Group
1000080088E31199
EFCMServer
Clients 2
Administrator

Figure 2-153 EFCM view by nickname

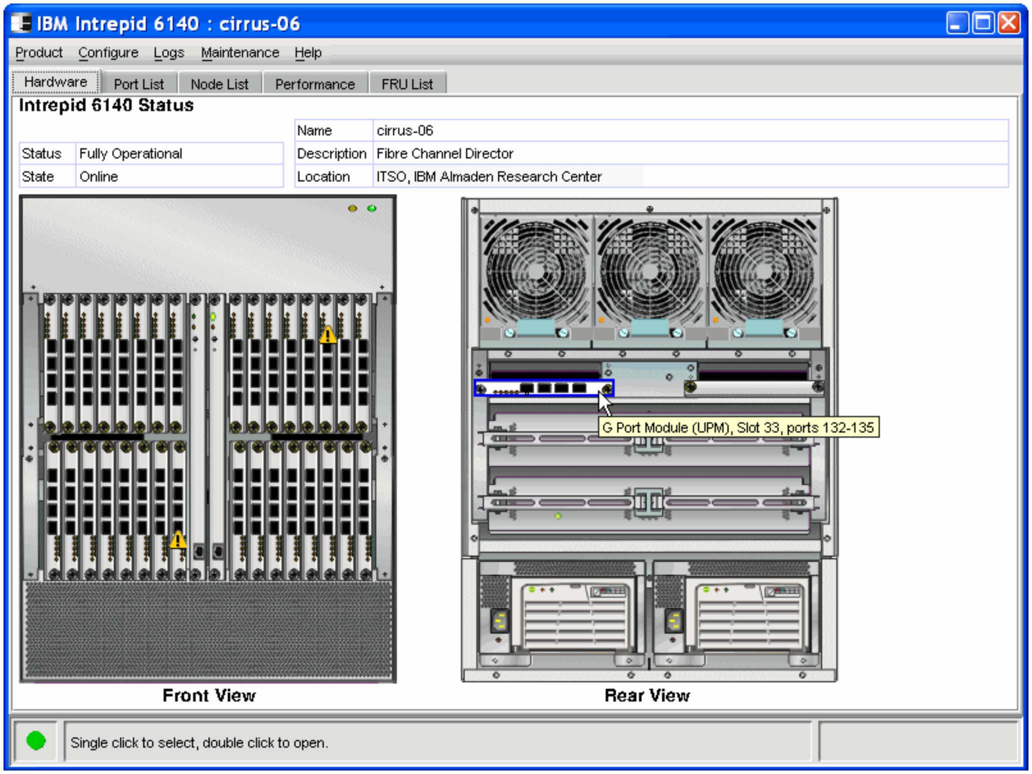
In some simple cases it might be tempting to work with the WWN and to skip or ignore the task of assigning nicknames. However, as more devices are attached, maintaining the fabric with names is more convenient and easier than figuring out which WWN belongs to which machine at a later date.

After assigning nicknames, the Node List View of the Element Manager shows the names of those that are currently attached. With a growing SAN, it becomes more and more important to be able to distinguish between the node ports.

Note: Nicknames are maintained by the EFCM server. Hence they are only usable within EFCM and Element Manager windows, and not the CLI or EFCM Basic Web GUI.

2.14.17 SAN140M interactive port card view

Unlike switches, directors use cards, or blades, to house the SFP optics in groups. For the SAN140M these are the four-port 2/4 Gbps UPM and the single-port 10 Gbps XPM cards. In the Element Manager *Hardware* default view shown in Figure 2-154, you see all the cards installed in the director. This also shows the Flyover Display feature, which causes descriptive text to appear when you hover your mouse cursor over the various parts, in this case the UPM card in slot 33 on the rear of the director.


IBM Intrepid 6140 : cirrus-06
Product
Configure
Logs
Maintenance
Help
Hardware
Port List
Node List
Performance
FRU List
Front View
Rear View

Intrepid 6140 Status

Status	Fully Operational
State	Online

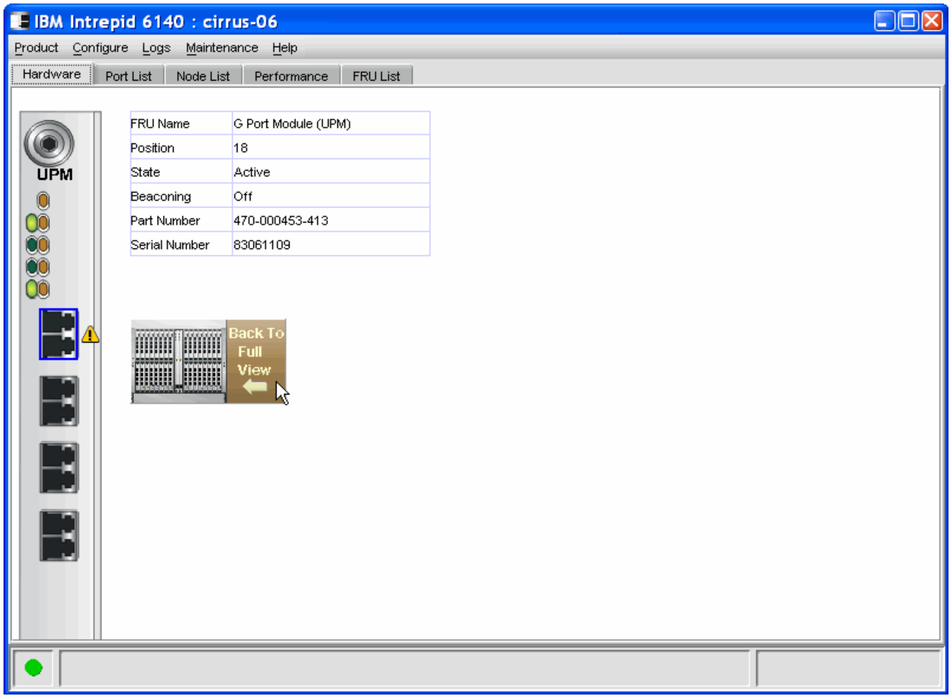
Name	cirrus-06
Description	Fibre Channel Director
Location	ITSO, IBM Almaden Research Center

G Port Module (UPM), Slot 33, ports 132-135

Single click to select, double click to open.

Figure 2-154 SAN140M Element Manager Hardware view

Double-clicking one of the port cards changes the view to show details of the single card, as shown in Figure 2-155. If you move your mouse over a port, its number appears. If you double-click a port, the Port Properties window displays.


IBM Intrepid 6140 : cirrus-06
Product Configure Logs Maintenance Help
Hardware Port List Node List Performance FRU List
UPM
Back To Full View

FRU Name	G Port Module (UPM)
Position	18
State	Active
Beaconing	Off
Part Number	470-000453-413
Serial Number	83061109

Figure 2-155 SAN140M single card view

To return to the view showing all the cards, click the button shown in Figure 2-156.

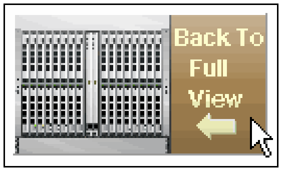

Back To
Full
View

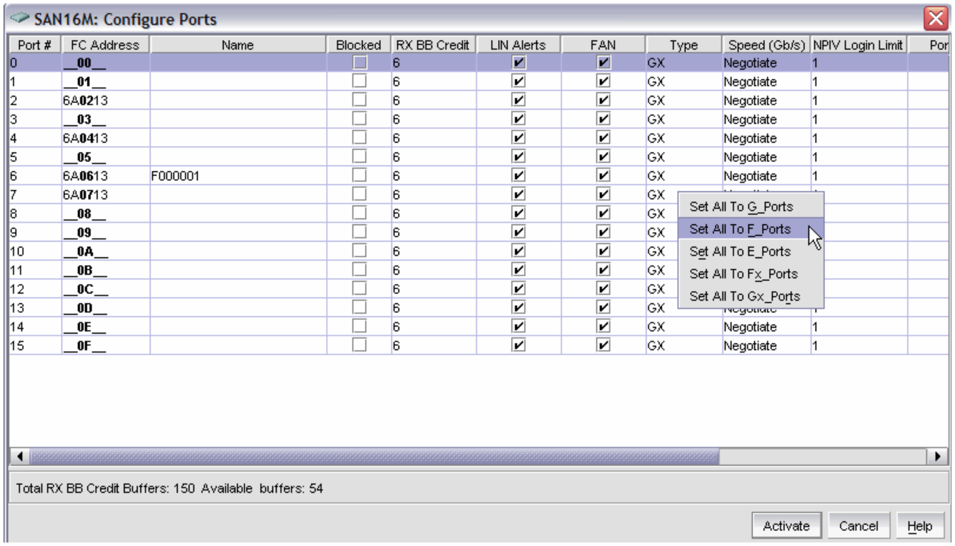
Figure 2-156 SAN140M back to full view

> **Note:** The same applies to the SAN256M 2027-256 director.

2.14.18 Arbitrated loop devices

Some devices, typically tape drives, can only operate in arbitrated loop (FC-AL) mode rather than as a switched fabric device. The SAN32M-1 switch and SAN140M director do not support direct attachment of FC-AL devices, so if you have to attach an FC-AL device, be sure to use one of the other members of the IBM m-type family.

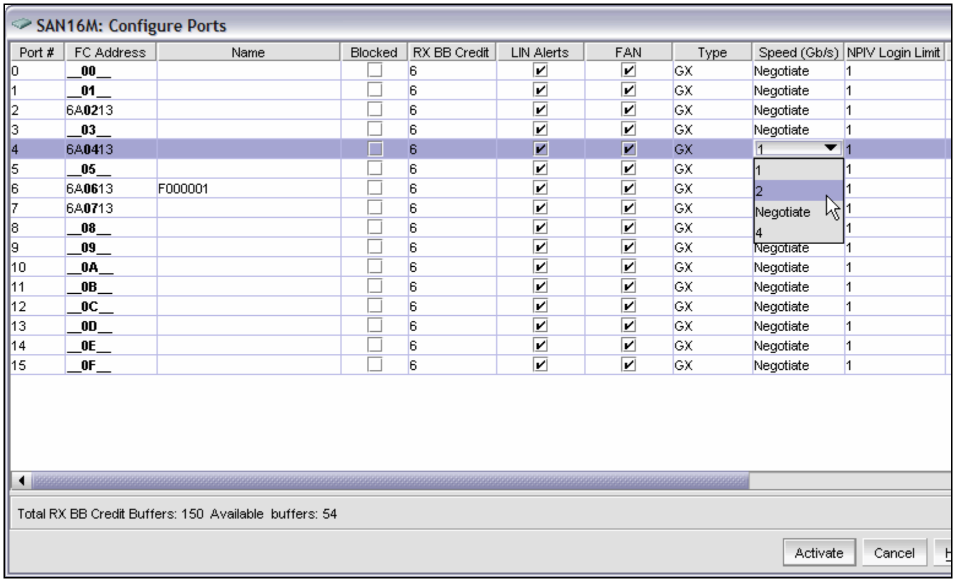
Some of the newer IBM tape drives, such as the 3592, support both switched fabric and arbitrated loop attachment. When the tape drive logs in to the switch port, by default they negotiate the best speed and connectivity method automatically. If you want, you can configure the switch port to only support fabric mode connections and only at specific speeds. This is done by selecting **Configure** → **Ports...** and clicking in the **Type** or **Speed** columns, and selecting from the drop-down lists, as shown in Figure 2-157 and Figure 2-158.



Port #	FC Address	Name	Blocked	RX BB Credit	LIN Alerts	FAN	Type	Speed (Gb/s)	NPIV Login Limit	Por
0	__00__		☐	6	☑	☑	GX	Negotiate	1	
1	__01__		☐	6	☑	☑	GX	Negotiate	1	
2	6A0213		☐	6	☑	☑	GX	Negotiate	1	
3	__03__		☐	6	☑	☑	GX	Negotiate	1	
4	6A0413		☐	6	☑	☑	GX	Negotiate	1	
5	__05__		☐	6	☑	☑	GX	Negotiate	1	
6	6A0613	F000001	☐	6	☑	☑	GX	Negotiate	1	
7	6A0713		☐	6	☑	☑	GX	Negotiate	1	
8	__08__		☐	6	☑	☑	GX			
9	__09__		☐	6	☑	☑	GX			
10	__0A__		☐	6	☑	☑	GX			
11	__0B__		☐	6	☑	☑	GX			
12	__0C__		☐	6	☑	☑	GX			
13	__0D__		☐	6	☑	☑	GX	Negotiate	1	
14	__0E__		☐	6	☑	☑	GX	Negotiate	1	
15	__0F__		☐	6	☑	☑	GX	Negotiate	1	

Total RX BB Credit Buffers: 150 Available buffers: 54

Figure 2-157 Setting port type



Port #	FC Address	Name	Blocked	RX BB Credit	LIN Alerts	FAN	Type	Speed (Gb/s)	NPIV Login Limit
0	__00__		☐	6	☑	☑	GX	Negotiate	1
1	__01__		☐	6	☑	☑	GX	Negotiate	1
2	6A0213		☐	6	☑	☑	GX	Negotiate	1
3	__03__		☐	6	☑	☑	GX	Negotiate	1
4	6A0413		☐	6	☑	☑	GX	1	1
5	__05__		☐	6	☑	☑	GX	1	1
6	6A0613	F000001	☐	6	☑	☑	GX	2	1
7	6A0713		☐	6	☑	☑	GX	Negotiate	1
8	__08__		☐	6	☑	☑	GX	4	1
9	__09__		☐	6	☑	☑	GX	Negotiate	1
10	__0A__		☐	6	☑	☑	GX	Negotiate	1
11	__0B__		☐	6	☑	☑	GX	Negotiate	1
12	__0C__		☐	6	☑	☑	GX	Negotiate	1
13	__0D__		☐	6	☑	☑	GX	Negotiate	1
14	__0E__		☐	6	☑	☑	GX	Negotiate	1
15	__0F__		☐	6	☑	☑	GX	Negotiate	1

Total RX BB Credit Buffers: 150 Available buffers: 54

Figure 2-158 Setting port speed

Port configuration options

The following port options are supported on those devices supporting FC-AL.

G_Port

Allows the port to auto-configure as an F_Port or an E_Port.

F_Port

Disables the E_Port and FL_Port function, so the port only connects to an N_Port.

E_Port

Only inter switch links (E_Port) are allowed.

Fx_Port

Allows the port to auto-configure as either an F_Port or an FL_Port, so the port only connects to an N_Port or NL_Port, and not an E_Port.

Gx_Port

This is the default option and it can auto-configure as F_Port, FL_Port or E_Port. The Gx_Port should always be the preferred port setting in order to connect an ISL, fabric node, or arbitrated loop public or private device. A private device can only be attached to a Gx_Port.

2.14.19 Persist fabric

Another feature of EFCM is *Persist Fabric*, which allows us to be notified of changes to the fabric, for example in the event of a switch or ISL failure. To turn on *Persist Fabric*, we right-click in the background area of the fabric display; this opens a context menu as shown in Figure 2-159.

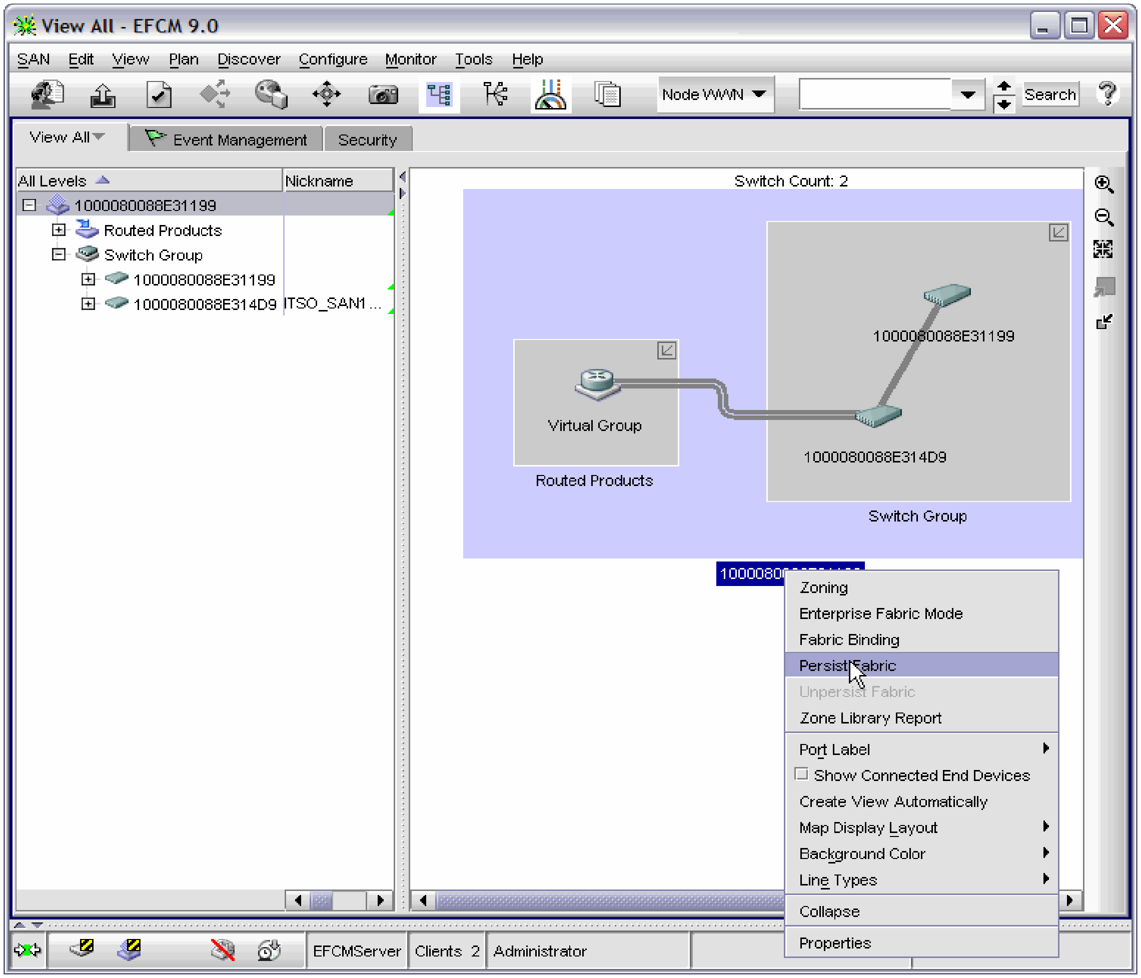
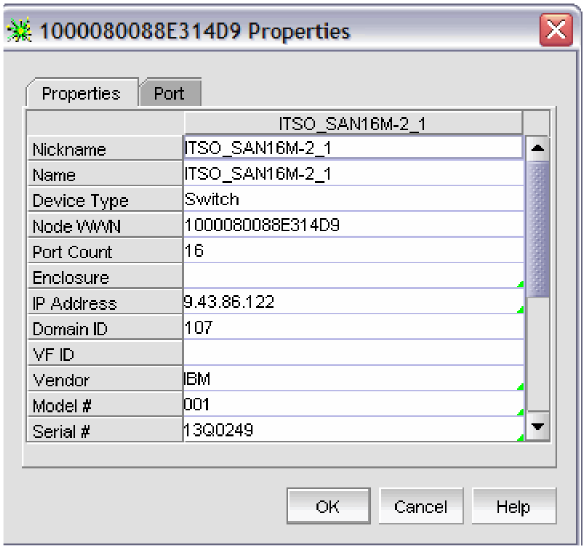

View All - EFCM 9.0
SAN Edit View Plan Discover Configure Monitor Tools Help
Node WWN
Search
View All
Event Management
Security
All Levels
Nickname
1000080088E31199
Routed Products
Switch Group
1000080088E31199
1000080088E314D9 ITSO_SAN1 ...
Switch Count: 2
Virtual Group
Routed Products
1000080088E31199
1000080088E314D9
Switch Group
Zoning
Enterprise Fabric Mode
Fabric Binding
Persist Fabric
Unpersist Fabric
Zone Library Report
Port Label
☐ Show Connected End Devices
Create View Automatically
Map Display Layout
Background Color
Line Types
Collapse
Properties
EFCMServer
Clients 2
Administrator

Figure 2-159 EFC Manager: Persist Fabric

We give the fabric a nickname by right-clicking and selecting **Properties**; in this case we call it *ITSO SAN16M-2_1*. This is also one of the ways to give each product a nickname by right-clicking and selecting **Properties**, as shown in Figure 2-160.



1000080088E314D9 Properties

	ITSO_SAN16M-2_1
Nickname	ITSO_SAN16M-2_1
Name	ITSO_SAN16M-2_1
Device Type	Switch
Node WWN	1000080088E314D9
Port Count	16
Enclosure	
IP Address	9.43.86.122
Domain ID	107
VF ID	
Vendor	IBM
Model #	001
Serial #	13Q0249

Figure 2-160 EFCM Manager: Product Nicknames

Notice that we have selected in the line below the menu bar to view our fabric by Nickname. Also notice that the persisted fabric has the letter P in the top left corner of the diagram, and a solid green circle in front of its name in the left pane.

Now, with Persist Fabric turned on, a failure of the ISL between our switches would be shown with the yellow triangle attention icon and the ISL changing to a broken yellow line, as shown in Figure 2-161.

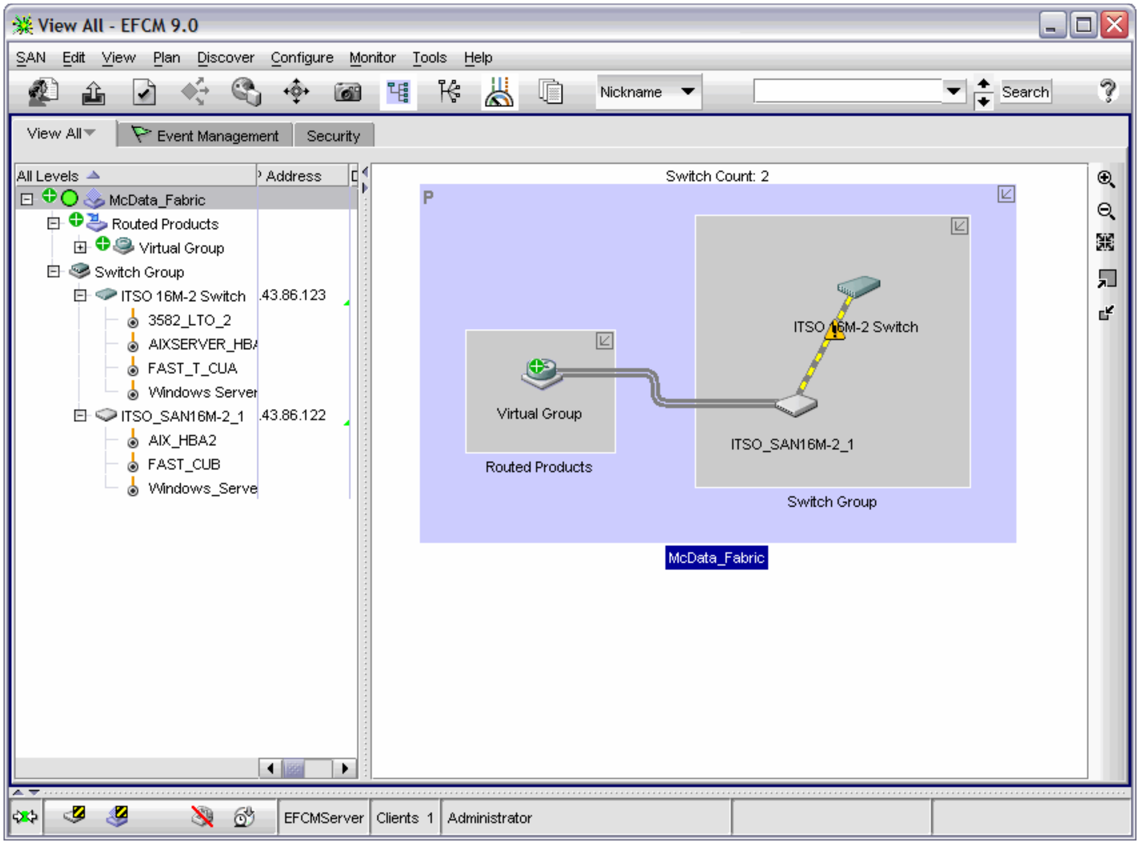

View All - EFCM 9.0
SAN Edit View Plan Discover Configure Monitor Tools Help
Nickname
Search
View All
Event Management
Security
All Levels
Address
McData_Fabric
Routed Products
Virtual Group
Switch Group
ITSO 16M-2 Switch
.43.86.123
3582_LTO_2
AIXSERVER_HBA
FAST_T_CUA
Windows Server
ITSO_SAN16M-2_1
.43.86.122
AIX_HBA2
FAST_CUB
Windows_Serve
Switch Count: 2
P
ITSO 16M-2 Switch
Virtual Group
ITSO_SAN16M-2_1
Routed Products
Switch Group
McData_Fabric
EFCMServer
Clients 1
Administrator

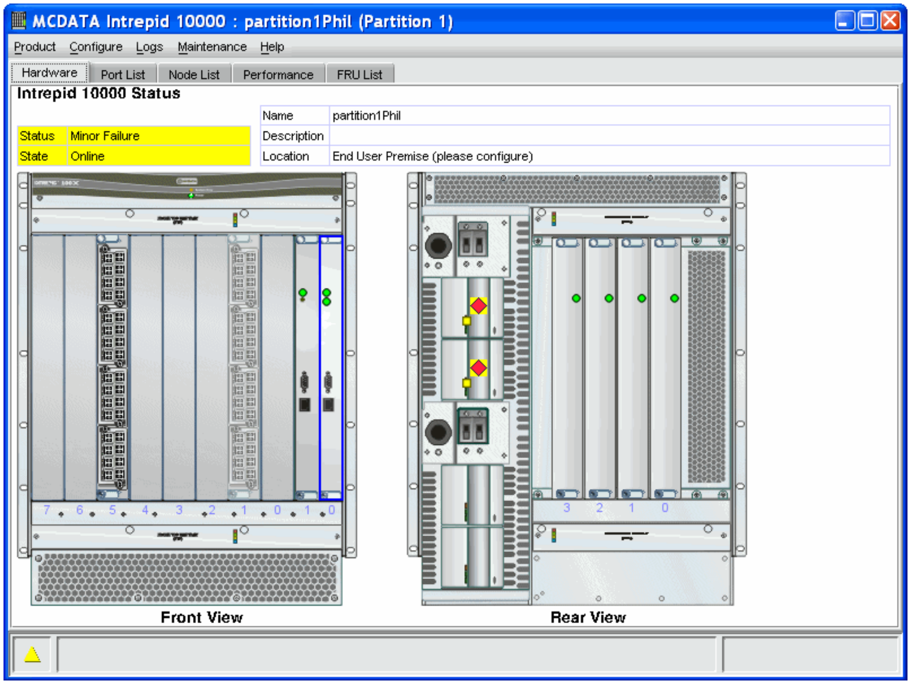
Figure 2-161 EFC Manager: broken ISL

Further detail of why the fabric failure occurred can be seen by selecting **Monitor** → **Logs** → **Fabric Log...** from the pull-down menu or by selecting the fabric icon in the lower left corner of EFC Manager.

2.15 Director partitioning

The IBM TotalStorage SAN256M director introduced the ability to partition a single physical director into up to four logical partitions, known as Director FlexPars. Each FlexPar acts like an independent director with its own fabric services, TCP/IP address, independent firmware and isolation of fabric events. Currently the unit of granularity for a partition is the line module (LIM), but the architecture is designed to provide granularity at the port level.

Figure 2-162 shows the Element Manager Hardware view for partition 1 of a SAN256M director. This director has two line modules installed, one in slot 1 and another in slot 5. The LIM in slot 1 is greyed out because it does not belong to this partition.


MCDATA Intrepid 10000 : partition1Phil (Partition 1)
Product
Configure
Logs
Maintenance
Help
Hardware
Port List
Node List
Performance
FRU List
7
6
5
4
3
2
1
0
1
0
3
2
1
0
Front View
Rear View

Intrepid 10000 Status

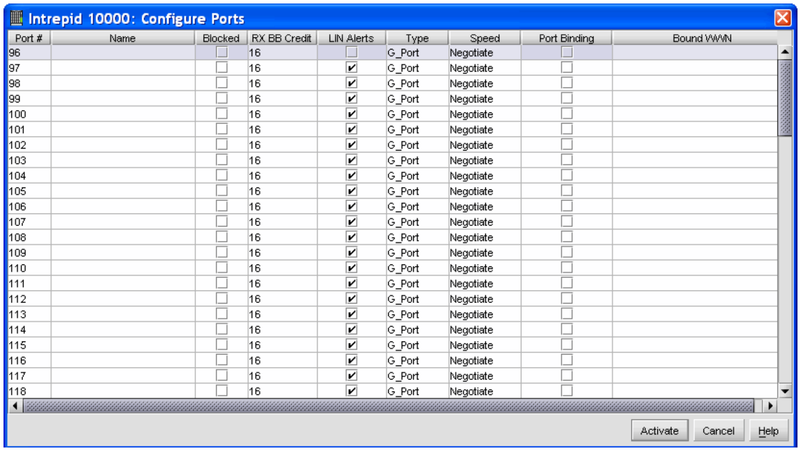
Status	Minor Failure
State	Online

Name	partition1Phil
Description	
Location	End User Premise (please configure)

Figure 2-162 SAN256M hardware view

Figure 2-162 also shows that the power supplies in positions 2 and 3 have a problem, hence the status of Minor Failure, and that all four switch modules (SWMs) are installed.

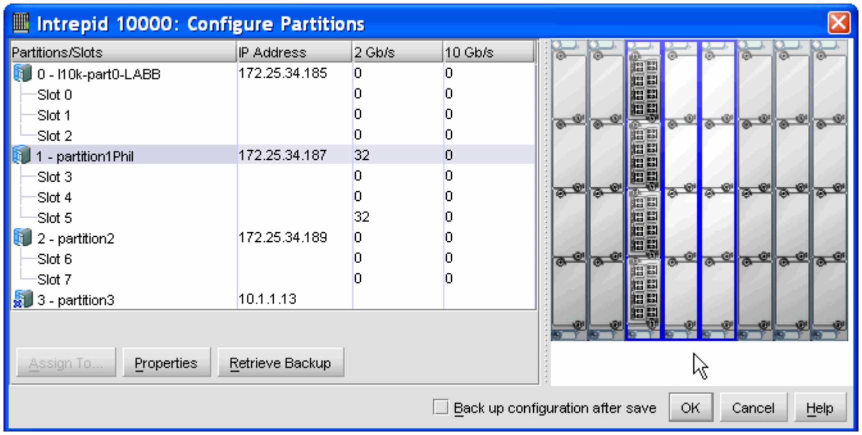
Operations performed on the SAN256M are the same as the other IBM m-type family devices, except that they are restricted to the current partition. As an example, selecting **Configure** → **Ports...** produces the window shown in Figure 2-163, and only shows the ports for the LIMs in the current partition.


Intrepid 10000: Configure Ports

Port #	Name	Blocked	RX BB Credit	LIN Alerts	Type	Speed	Port Binding	Bound WWN
96		☐	16	☐	G_Port	Negotiate	☐	
97		☐	16	☑	G_Port	Negotiate	☐	
98		☐	16	☑	G_Port	Negotiate	☐	
99		☐	16	☑	G_Port	Negotiate	☐	
100		☐	16	☑	G_Port	Negotiate	☐	
101		☐	16	☑	G_Port	Negotiate	☐	
102		☐	16	☑	G_Port	Negotiate	☐	
103		☐	16	☑	G_Port	Negotiate	☐	
104		☐	16	☑	G_Port	Negotiate	☐	
105		☐	16	☑	G_Port	Negotiate	☐	
106		☐	16	☑	G_Port	Negotiate	☐	
107		☐	16	☑	G_Port	Negotiate	☐	
108		☐	16	☑	G_Port	Negotiate	☐	
109		☐	16	☑	G_Port	Negotiate	☐	
110		☐	16	☑	G_Port	Negotiate	☐	
111		☐	16	☑	G_Port	Negotiate	☐	
112		☐	16	☑	G_Port	Negotiate	☐	
113		☐	16	☑	G_Port	Negotiate	☐	
114		☐	16	☑	G_Port	Negotiate	☐	
115		☐	16	☑	G_Port	Negotiate	☐	
116		☐	16	☑	G_Port	Negotiate	☐	
117		☐	16	☑	G_Port	Negotiate	☐	
118		☐	16	☑	G_Port	Negotiate	☐	

Figure 2-163 Ports for current partition

Selecting **Configure** → **Partitions** produces the window shown in Figure 2-164. In this example partition 1 is selected, and LIM slots 3, 4 and 5 are highlighted.

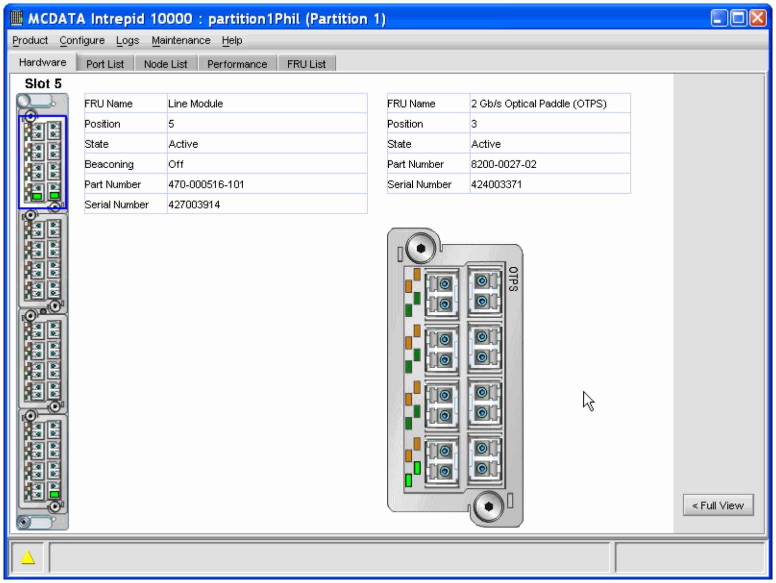

Intrepid 10000: Configure Partitions

Partitions/Slots	IP Address	2 Gb/s	10 Gb/s
0 - I10k-part0-LABB	172.25.34.185	0	0
Slot 0		0	0
Slot 1		0	0
Slot 2		0	0
1 - partition1Phil	172.25.34.187	32	0
Slot 3		0	0
Slot 4		0	0
Slot 5		32	0
2 - partition2	172.25.34.189	0	0
Slot 6		0	0
Slot 7		0	0
3 - partition3	10.1.1.13		

Figure 2-164 SAN256M Configure Partitions

To assign an unused LIM to a partition, highlight the LIM (or LIMs) in the left pane and click the **Assign To...** button. In the Assign Slots dialog box that displays, select the partition you want to assign the LIM to and click **OK**. Click **OK** in the Configure Partitions window to finish. If you check the **Back up configuration after save** check box, the partition configuration is backed up to the management server.

Double-clicking a LIM in the Hardware view changes the view to that shown in Figure 2-165. You can then click one of the four paddles to select which is shown in detail on the right-hand side of the window.

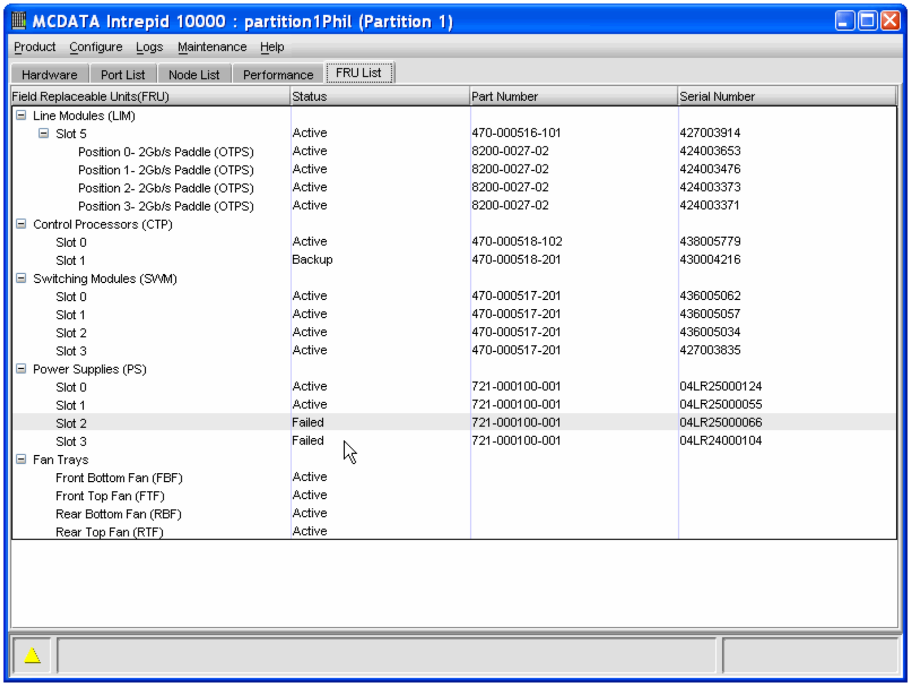

MCDATA Intrepid 10000 : partition1Phil (Partition 1)
Product
Configure
Logs
Maintenance
Help
Hardware
Port List
Node List
Performance
FRU List
Slot 5
OTPS
< Full View

FRU Name	Line Module
Position	5
State	Active
Beaconing	Off
Part Number	470-000516-101
Serial Number	427003914

FRU Name	2 Gb/s Optical Paddle (OTPS)
Position	3
State	Active
Part Number	8200-0027-02
Serial Number	424003371

Figure 2-165 SAN256M LIM and paddle view

Figure 2-166 shows the FRU List view, which gives details of all the FRUs for the current partition, including the two failed power supplies in this example.



Field Replaceable Units(FRU)	Status	Part Number	Serial Number
Line Modules (LIM)			
Slot 5	Active	470-000516-101	427003914
Position 0- 2Gb/s Paddle (OTPS)	Active	8200-0027-02	424003653
Position 1- 2Gb/s Paddle (OTPS)	Active	8200-0027-02	424003476
Position 2- 2Gb/s Paddle (OTPS)	Active	8200-0027-02	424003373
Position 3- 2Gb/s Paddle (OTPS)	Active	8200-0027-02	424003371
Control Processors (CTP)			
Slot 0	Active	470-000518-102	438005779
Slot 1	Backup	470-000518-201	430004216
Switching Modules (SWM)			
Slot 0	Active	470-000517-201	436005062
Slot 1	Active	470-000517-201	436005057
Slot 2	Active	470-000517-201	436005034
Slot 3	Active	470-000517-201	427003835
Power Supplies (PS)			
Slot 0	Active	721-000100-001	04LR25000124
Slot 1	Active	721-000100-001	04LR25000055
Slot 2	Failed	721-000100-001	04LR25000066
Slot 3	Failed	721-000100-001	04LR24000104
Fan Trays			
Front Bottom Fan (FBF)	Active		
Front Top Fan (FTF)	Active		
Rear Bottom Fan (RBF)	Active		
Rear Top Fan (RTF)	Active		

Figure 2-166 SAN256M FRU List

2.16 Zoning

In the topics that follow we discuss zoning — its purpose and implementation.

2.16.1 Why we require zoning

Zoning is the technique used to control access between end ports in a fabric. It controls which hosts can see which storage ports, and also protects hosts and their storage from each other. Without zoning it is difficult to guarantee data integrity, security, high availability, and fabric stability.

2.16.2 Zoning implementation

IBM m-type switches support zoning by WWN or port number, or a combination of the two. Zoning is enforced at the frame level by route tables in the hardware (ASIC). If a source port is not a member of the same zone as the destination port, then the routing table for that port is disabled and communication between the two is denied at the entry port.

When a device attempts to communicate with a destination device outside of its zone by sending a PLOGI, the frame is blocked. A Class 2 frame gets the fabric rejected, and a Class 3 frame is dropped.

2.16.3 Zoning recommendations

There are a number of ways one can zone a fabric, but there are no single correct way, there are incorrect ways. To make a decision on how to zone your fabric, you have to understand different zoning methods.

Common host zoning

Common host zoning is normally associated with small single fabric environments where it is the most common zoning schema. This has a zone per operating system, server manufacturer or HBA brand, or some similar approach.This offers a fairly simple approach. For example, NTservers operate well with each other. QLogic's HBAs operate well together. You then have a zone consisting of all the common servers, plus the storage devices they have to access.

Single target multiple initiator zoning

Traditionally, many storage subsystems had a rule that any port on an array could only be accessed by multiple servers using the same operating system. Administrators who started with the common host approach, but then wanted better granularity in their zoning, saw the benefit of having each zone consisting of one port on one storage array with all the devices that were allowed to access that port. This also made it visibly easy with zoning to monitor that they were following the arrays operating system support guidelines

Single initiator multiple target zoning

Increasingly common in heterogeneous SANs, this approach comes from a simple premise — SCSI initiators (servers) do not have to talk to other SCSI initiators. Therefore, a very robust approach to avoid any potential problems with servers upsetting each other is to have one server or indeed only one HBA in any zone, and then also put into that zone all the storage devices that the host is allowed to talk to. This is the most commonly recommended method of zoning for most SAN fabrics

Single initiator single target zoning

This is the ultimate in security, as we are keeping our zones to their absolute usable minimum size and so providing maximum security from our zoning. This has been used very successful in a few cases but is not so common. Without good software it is hard work to set up and manage.

Summary

The method you select to do your zoning depends as much on your technology as how you operate. You should carefully consider the different options and, choose an approach and use it. Remember, zoning is not the answer to all your problems. But it is a vital part of storage provisioning. Starting off correctly, even if you think it is overkill in a small SAN, allows you to continue in the future with a reliable and robust SAN.

2.16.4 Zone member definitions

A zone's members are specified either by the switch port number (and with it, the node ports connected to it), by the WWPN of a node port, by Fabric Address, or by a mixture of all. Note that WWNNs are not used for zoning definitions.

Zone member definition by WWPN

The major advantage with WWPN based zoning is that it provides the flexibility to move any device from one port to another port and it still retains its zone membership. This is useful when rearranging ports or moving to a spare port because of a port failure. The disadvantage is that removing or replacing a device HBA, and thus changing its WWPN, disrupts zone operation and could incorrectly exclude or include devices until the zone is re-configured with the new WWPN.

Note: Some devices such as the IBM TotalStorage Enterprise Storage Server avoid this problem by effectively preserving the WWPN on the replacement host adapters.

In order to make it easy to reconfigure WWN or nicknames in affected zones, there are Find, Remove, and Replace WWN/Nickname dialog boxes available among the Zoning Tasks.

Tip: Assigning nicknames to WWPNs greatly simplifies zoning.

A WWPN can belong to multiple zones.

Zone member definition by switch port number

Port based zoning is also known as static zoning. It consists of specifying the domain and the port number of the switch to be added to the zone.

By using port numbers to define zone members, any device attached to that port can connect to the others in the same zone. This has the advantage that we do not have to worry about redefining the WWPN if an HBA has to be replaced. A disadvantage is that someone could rearrange the port connections to allow the possibility of gaining access to devices that you did not intend them to have access to, and losing access to correct devices.

To provide a higher level of security, you can also configure the port binding feature to bind a WWN to a given port. By doing this, you do not allow any other device to plug into the port. See 2.17.3, "Port Binding" on page 566 for more details.

A single port can also be a member of multiple zones.

Restriction: The default zone cannot be used in Open Fabric interop mode.

Default zone

The *default zone* is defined as "a zone that contains all attached devices that are not members of a separate active zone", and can be activated independently of zone sets. This means that if the active zone set is disabled, and the default zone is enabled, then all devices are effectively in one zone. If the default zone is disabled and no zone set is active, no node ports can communicate.

Restriction: The default zone cannot be used in Open Fabric interop mode.

Tip: We recommend that the default zone always be disabled.

Safe zoning mode

A new feature called *safe zoning mode*, which is enabled by default, prevents a default zone from being enabled in McDATA Fabric Mode, which might lead to problems in a fabric if zones are accidentally removed or new unzoned devices are added to the fabric.

It also helps protect against unintentional fabric merges by performing extra zone set checks when fabrics are connected.

2.16.5 Zone management with zone sets

From within the McDATA EFCM, we can specify up to 64 zone sets in the zone library. This is purely an EFCM limitation, not a device one. A zone set consists of one or more zones that can be activated and deactivated at the same time. See Table 2-3 on page 391 for other zoning limits.

Only one zone set can be active at one time. Activating an inactive zone set deactivates the previously active zone set.

There can be multiple zone sets configured for different tasks, for example if we want to have certain node ports in the same zone for backup, but not during normal operation.

It is always wise to be careful when activating zone sets, as any one of the following events could occur, whether by design or by accident:

- When the default zone is disabled, the devices that are not members of the active zone set become isolated and cannot communicate.
- When no zone set is active, then all devices are considered to be in the default zone. If no zone set is active and default zone is disabled, then no device can communicate.
- Activating a new zone set replaces the currently active zone set. Be sure you have the correct zone set for the fabric you are currently updating, if your EFC Manager manages multiple fabrics.

> **Note:** EFC Manager provides a feature which provides a difference check against the currently active zone set. Any differences are highlighted to alert you of any potential inconsistencies. This should help eliminate the chance of an incorrect zone set activation.

- Deactivating the currently active zone set makes all devices members of the default zone if default zoning is enabled. If default zoning is disabled, all communication stops.
- Zones defined through the EFCM are saved in a zone library. Any zone in the zone library can be displayed, modified, and selected to be part of a zone set.

> **Tip:** It is strongly recommended that all devices be properly zoned, and the default zone set disabled, because this improves fabric security.

Zone change notification

A fabric format Registered State Change Notification (RSCN) service request is sent to all N_Ports when the zoning configuration is changed, unless you check the **Suppress RSCN’s on zone set activations** option in the Switch Operating Parameters dialogue box. Normally such notifications should be allowed.

Broadcast frames are transmitted to all N_Ports, regardless of the zone to which they belong.

Our zoning example

An example of how zones and zone sets are related is shown in Figure 2-167.

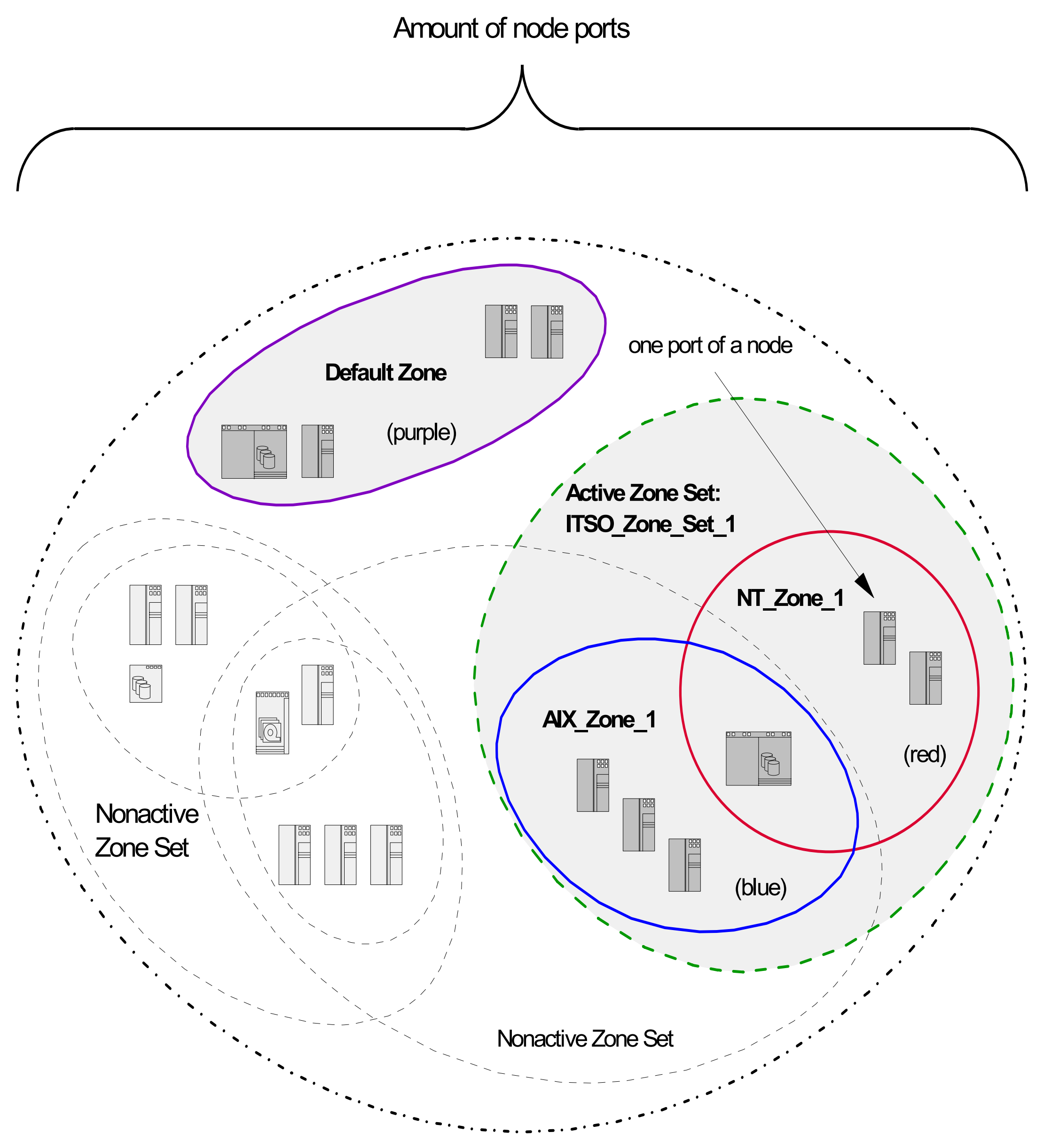

Amount of node ports
Default Zone
(purple)
one port of a node
Active Zone Set:
ITSO_Zone_Set_1
NT_Zone_1
AIX_Zone_1
(red)
(blue)
Nonactive
Zone Set
Nonactive Zone Set

Figure 2-167 Relationship of zone sets, zones, the default zone and node ports

The node symbols here (from servers and from the ESS), represent one or more node ports and not necessarily the whole FC node with all ports. For example, all three ESS symbols could be ports of the same ESS.

The solid (blue, red, and purple) areas represent areas where traffic is permitted. The blue and the red zones represent the AIX and the NT zones to be defined in this topic. The dotted green line around the two zones represents the active zone set.

The purple area is the default zone. In this example the default zone is enabled, which makes it possible for all node ports which are not configured in a zone of the currently active zone set to communicate with each other. For anything other than the simplest fabric, it is strongly recommended that the default zone be disabled to improve security.

Zoning and LUN masking

Zoning allows us to specify which ports can connect to each other. When we are connecting to storage arrays or storage subsystems, like the IBM TotalStorage Enterprise Storage Server®, with multiple LUNs defined, we still have to perform LUN masking at the storage subsystem level, so each host is only allowed to access its own LUNs.

2.16.6 Zoning with EFCM

The initial view from EFCM shows the topology of existing fabrics. The fabrics are listed on the left side of the view, and linked to the Fabric name are the products making up the highlighted fabric as shown in Figure 2-168. Note that in this example we have two fabrics, and we have selected the first fabric, which is comprised of three products.

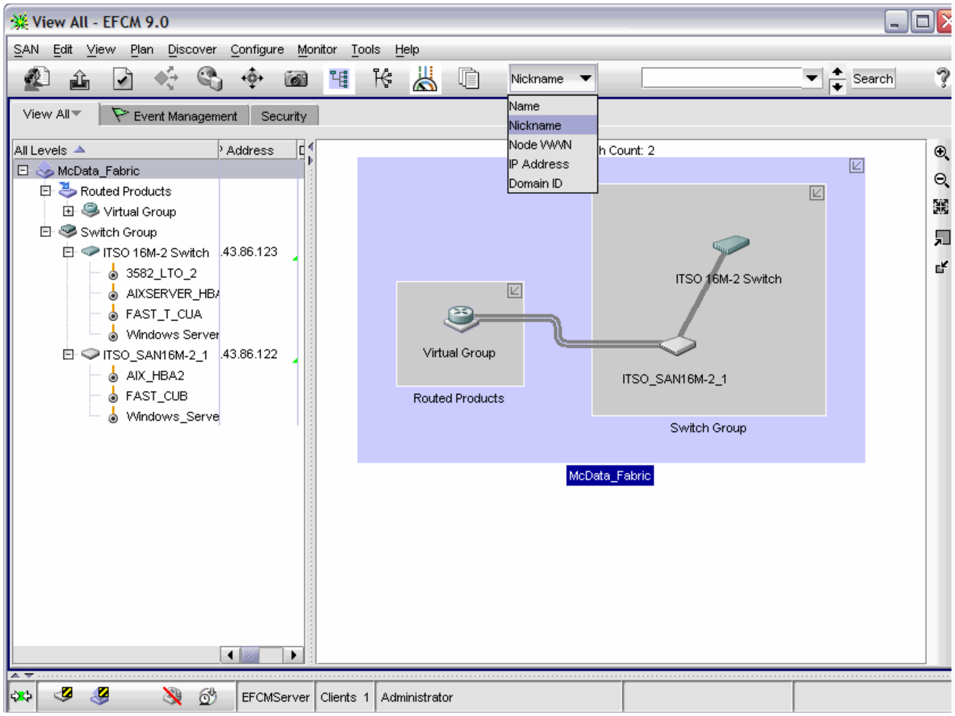

View All - EFCM 9.0
SAN
Edit
View
Plan
Discover
Configure
Monitor
Tools
Help
Nickname
Search
Name
Nickname
Node WWN
IP Address
Domain ID
View All
Event Management
Security
All Levels
Address
McData_Fabric
Routed Products
Virtual Group
Switch Group
ITSO 16M-2 Switch
.43.86.123
3582_LTO_2
AIXSERVER_HBA
FAST_T_CUA
Windows Server
ITSO_SAN16M-2_1
.43.86.122
AIX_HBA2
FAST_CUB
Windows_Serve
h Count: 2
ITSO 16M-2 Switch
Virtual Group
Routed Products
ITSO_SAN16M-2_1
Switch Group
McData_Fabric
EFCMServer
Clients 1
Administrator

Figure 2-168   EFC Manager fabric view

As also shown in Figure 2-168, fabrics and devices can be viewed by Name, Nickname, Node Name, IP Address, or Domain ID.

2.16.7 The Zoning Dialog Box

To view details of the fabrics, zone sets, zones and members, or to make changes we invoke the zoning dialog window by selecting **Configure** → **Zoning...**, as shown in Figure 2-169.

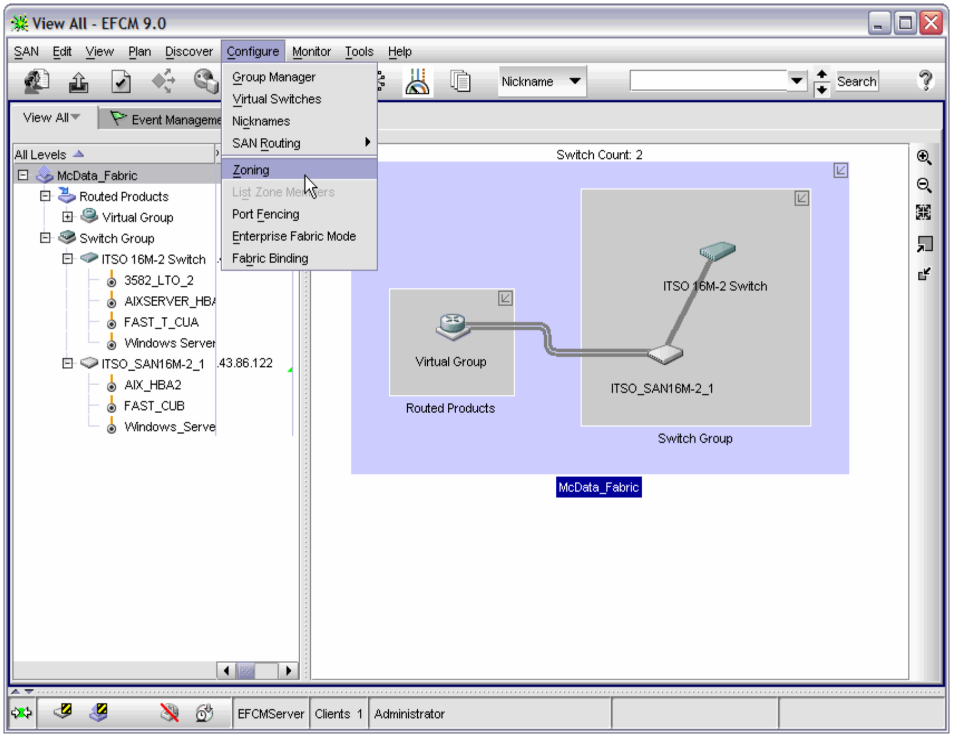

View All - EFCM 9.0
SAN
Edit
View
Plan
Discover
Configure
Monitor
Tools
Help
Group Manager
Virtual Switches
Nicknames
SAN Routing
Zoning
List Zone Members
Port Fencing
Enterprise Fabric Mode
Fabric Binding
Nickname
Search
View All
Event Management
All Levels
McData_Fabric
Routed Products
Virtual Group
Switch Group
ITSO 16M-2 Switch
3582_LTO_2
AIXSERVER_HBA
FAST_T_CUA
Windows Server
ITSO_SAN16M-2_1
.43.86.122
AIX_HBA2
FAST_CUB
Windows_Serve
Switch Count: 2
ITSO 16M-2 Switch
Virtual Group
ITSO_SAN16M-2_1
Routed Products
Switch Group
McData_Fabric
EFCMServer
Clients 1
Administrator

Figure 2-169 Initiating the Zoning dialog window

This brings up the Zoning dialog window shown in Figure 2-170.

We use the zoning dialog window to accomplish the following tasks:

- View fabric zones and members
- Move members to and from zones
- Create zones and zone sets
- Move zones to and from zone sets
- Activate and deactivate zone sets
- Enable or disable the default zone
- Import or export zone libraries

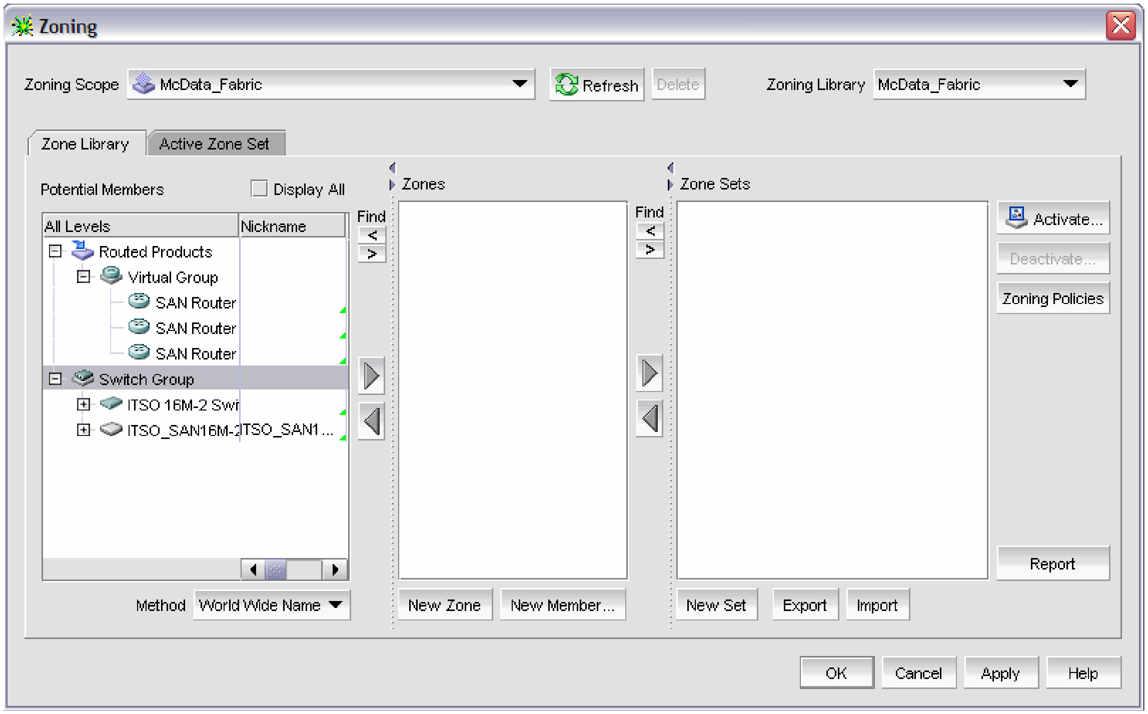

Zoning
Zoning Scope
McData_Fabric
Refresh
Delete
Zoning Library
McData_Fabric
Zone Library
Active Zone Set
Potential Members
Display All
All Levels
Nickname
Routed Products
Virtual Group
SAN Router
SAN Router
SAN Router
Switch Group
ITSO 16M-2 Swi
ITSO_SAN16M-2 ITSO_SAN1...
Find
Zones
Find
Zone Sets
Activate...
Deactivate...
Zoning Policies
Report
Method
World Wide Name
New Zone
New Member...
New Set
Export
Import
OK
Cancel
Apply
Help

Figure 2-170 Zoning dialog window

2.16.8 Zones, zone sets, and zoning

As an example, we go through the process of creating zones, adding members to a zone, and creating zone sets for the zones. First we again initiate the Zoning dialog window, by selecting **Configure** → **Zoning...** from the EFCM.

Creating a new zone

We have to create at least one zone to go in our zone set. We select New Zone under the **Zones** window and type a name, for this example we use the name AIX_Zone_1, as shown in Figure 2-171. We repeat these steps to create more zones for use in later examples.

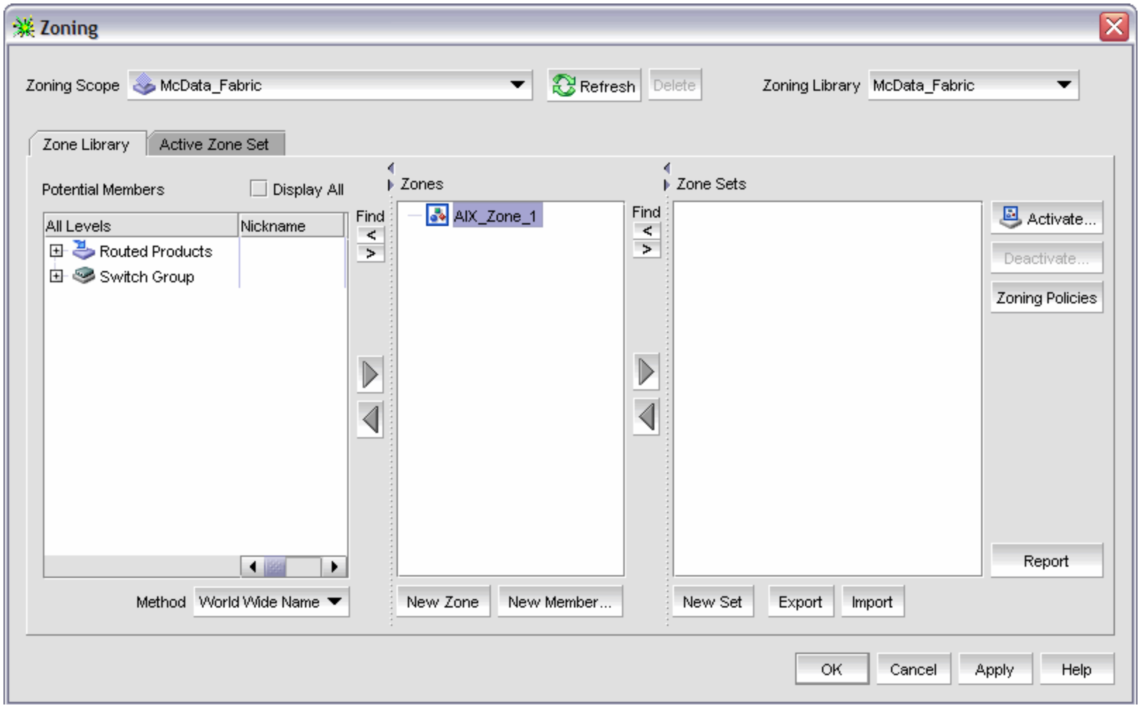

Zoning
Zoning Scope
McData_Fabric
Refresh
Delete
Zoning Library
McData_Fabric
Zone Library
Active Zone Set
Potential Members
☐ Display All
All Levels
Nickname
Routed Products
Switch Group
Find
<
>
Zones
AIX_Zone_1
Find
<
>
Zone Sets
Activate...
Deactivate...
Zoning Policies
Report
Method
World Wide Name
New Zone
New Member...
New Set
Export
Import
OK
Cancel
Apply
Help

Figure 2-171 Zoning dialog window: Zone creation

Adding members to the zone

In the Zoning dialog window, the left-most column, labeled Potential Zone Members, displays the available devices and their ports. Here we can view all of the WWPNs or nicknames of the connected FC ports. Here we have to be very careful (in a multi-fabric environment) that we choose the correct fabric we want to work on.

This can be selected by clicking the drop-down menu in the upper left corner, as shown in Figure 2-172. In this example we view the fabrics by nickname.

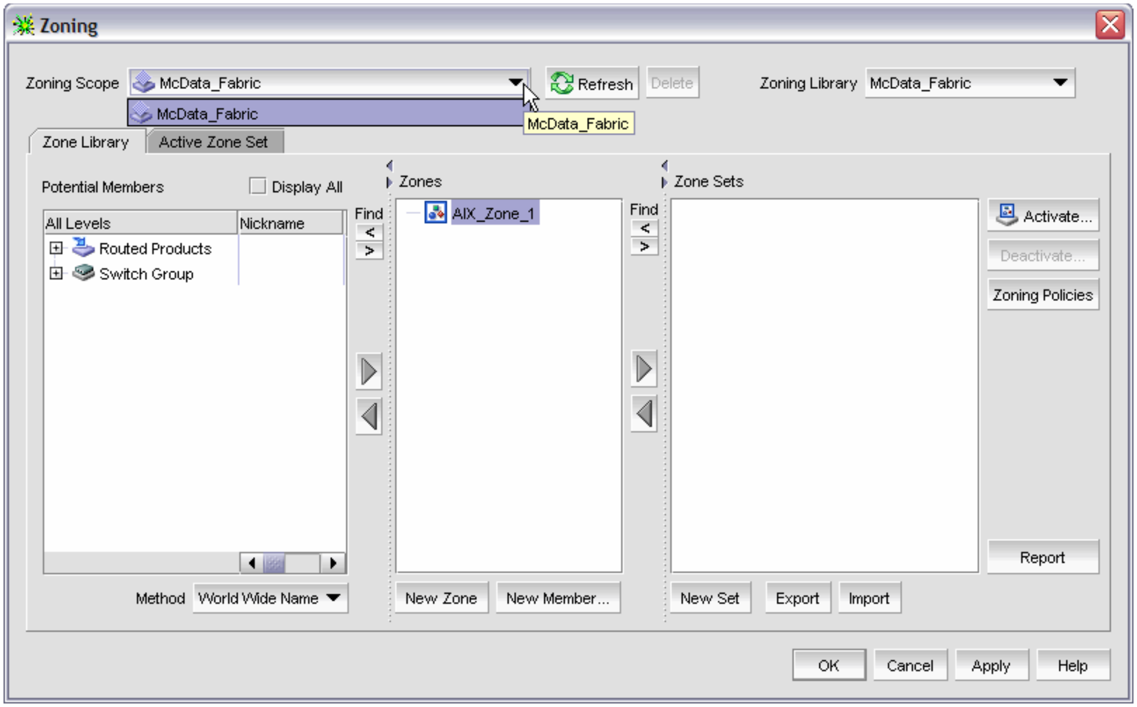

Zoning
Zoning Scope
McData_Fabric
McData_Fabric
McData_Fabric
Refresh
Delete
Zoning Library
McData_Fabric
Zone Library
Active Zone Set
Potential Members
Display All
All Levels
Nickname
Routed Products
Switch Group
Find
Zones
AIX_Zone_1
Find
Zone Sets
Activate...
Deactivate...
Zoning Policies
Report
Method
World Wide Name
New Zone
New Member...
New Set
Export
Import
OK
Cancel
Apply
Help

Figure 2-172 Zoning dialog window: Fabric choice

Below the left column there is a drop-down list with two choices. Here we can choose if we want to zone by WWN, Domain/Port, or Fabric Address.

Note: WWN is the only method to be used for Router fabrics

To add members to the zone we created, we select the WWN on the left. We select the zone we want to add to in the middle column, and then click the right-arrow between them to add the selected member to the selected zone as illustrated in Figure 2-173.

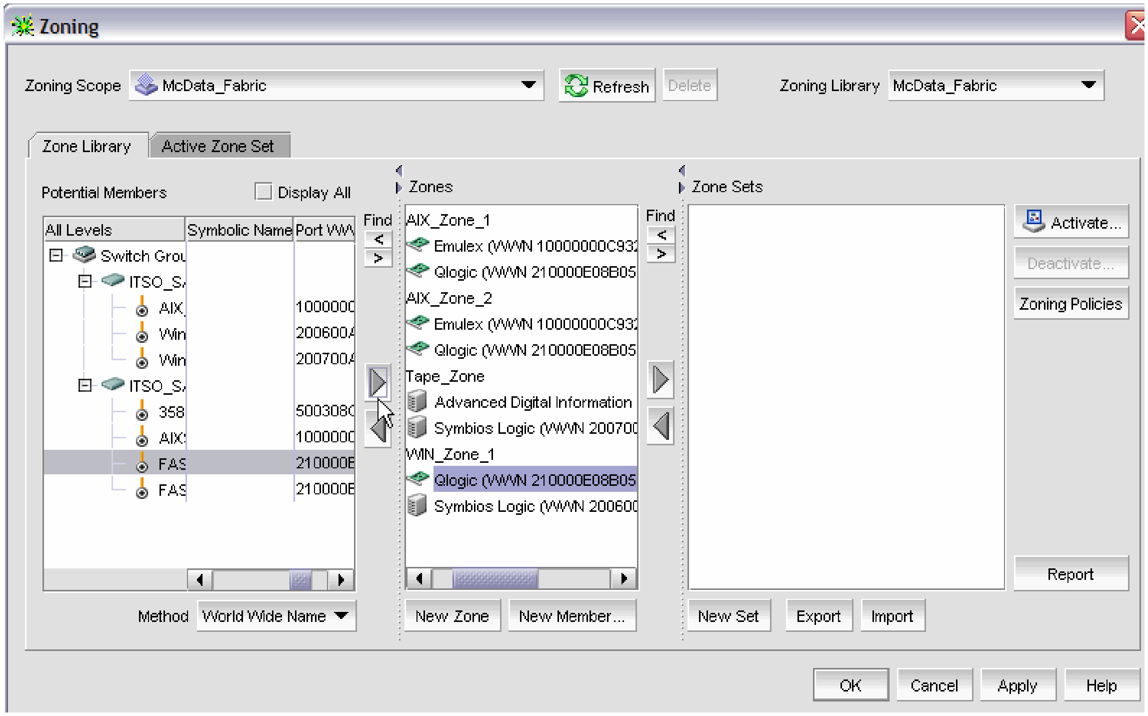
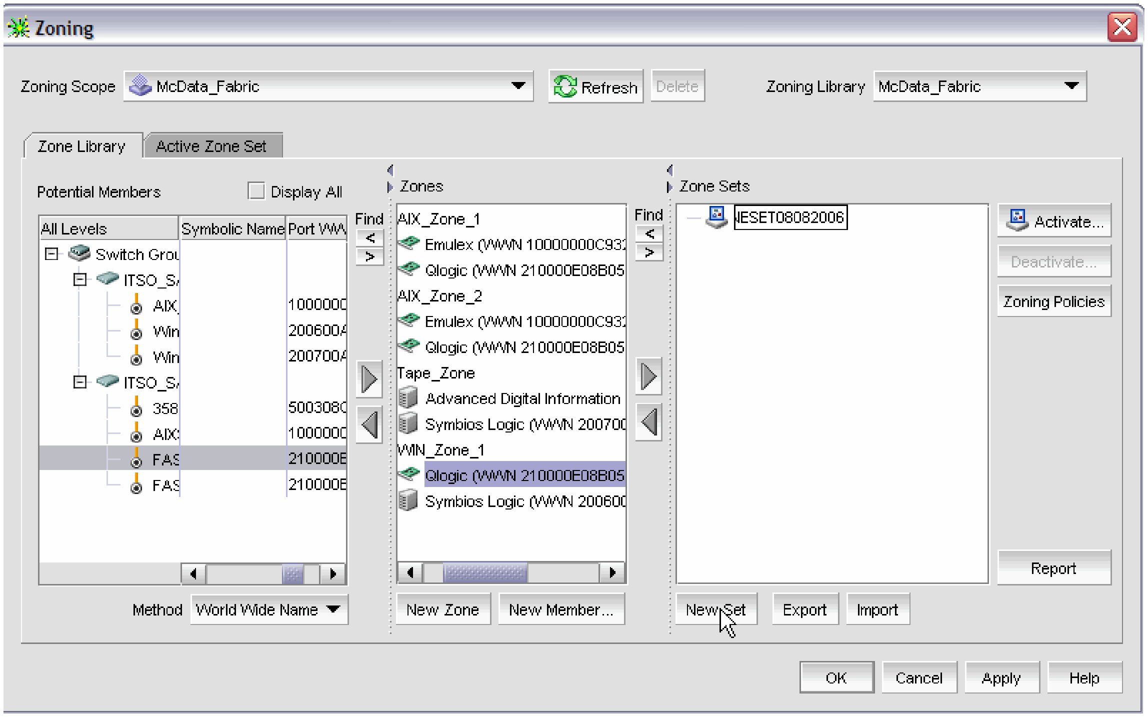

Zoning
Zoning Scope
McData_Fabric
Refresh
Delete
Zoning Library
McData_Fabric
Zone Library
Active Zone Set
Potential Members
Display All
All Levels
Symbolic Name
Port WW
Switch Grou
ITSO_S
Find
Zones
AIX_Zone_1
Emulex (WWN 10000000C93
Qlogic (WWN 210000E08B05
AIX_Zone_2
Emulex (WWN 10000000C93
Qlogic (WWN 210000E08B05
Tape_Zone
Advanced Digital Information
Symbios Logic (WWN 20070
WIN_Zone_1
Qlogic (WWN 210000E08B05
Symbios Logic (WWN 20060
Zone Sets
Activate...
Deactivate...
Zoning Policies
Report
Method
World Wide Name
New Zone
New Member...
New Set
Export
Import
OK
Cancel
Apply
Help

Figure 2-173 Zoning Dialog Box: Adding members to zone

We repeat these steps for this example and create other zones named AIX_ZONE_2, WIN_Zone_1, and Tape_Zone

Creating a new zone set

Because there are no zone sets in the library, we have to create one. To create a new zone set from the Zoning dialog window we select **New Set** under the Zone Sets column and type in a name for our new zone set as shown in Figure 2-174.


Zoning Scope McData_Fabric

Zoning Library McData_Fabric

Method World Wide Name

Zone Sets: NESET08082006

Zoning
Refresh
Delete
Zone Library
Active Zone Set
Potential Members
☐ Display All
All Levels
Symbolic Name
Port WW
Switch Grou
ITSO_S
AIX
Win
Win
ITSO_S
358
AIX
FAS
FAS
1000000
200600
200700
500308
1000000
210000E
210000E
Find
<
>
Zones
AIX_Zone_1
Emulex (WWN 10000000C93
Qlogic (WWN 210000E08B05
AIX_Zone_2
Emulex (WWN 10000000C93
Qlogic (WWN 210000E08B05
Tape_Zone
Advanced Digital Information
Symbios Logic (WWN 200700
WIN_Zone_1
Qlogic (WWN 210000E08B05
Symbios Logic (WWN 200600
New Zone
New Member...
Find
<
>
Zone Sets
New Set
Export
Import
Activate...
Deactivate...
Zoning Policies
Report
OK
Cancel
Apply
Help

Figure 2-174 Zoning dialog window: Zone set creation

We recommend that you use a zoneset name that you can use to determine which zoneset was the last used. This would be useful if you have to go back to a previous zoneset or you configure zonesets for particular uses. Putting the date stamp inside the name has been found to be useful.

When we have a zone that contains at least one member, we can add that zone to a zone set with the same steps we used to add members to the zone. First highlight the zone, then select the zone set in the right column and click the right-arrow as shown in Figure 2-175.

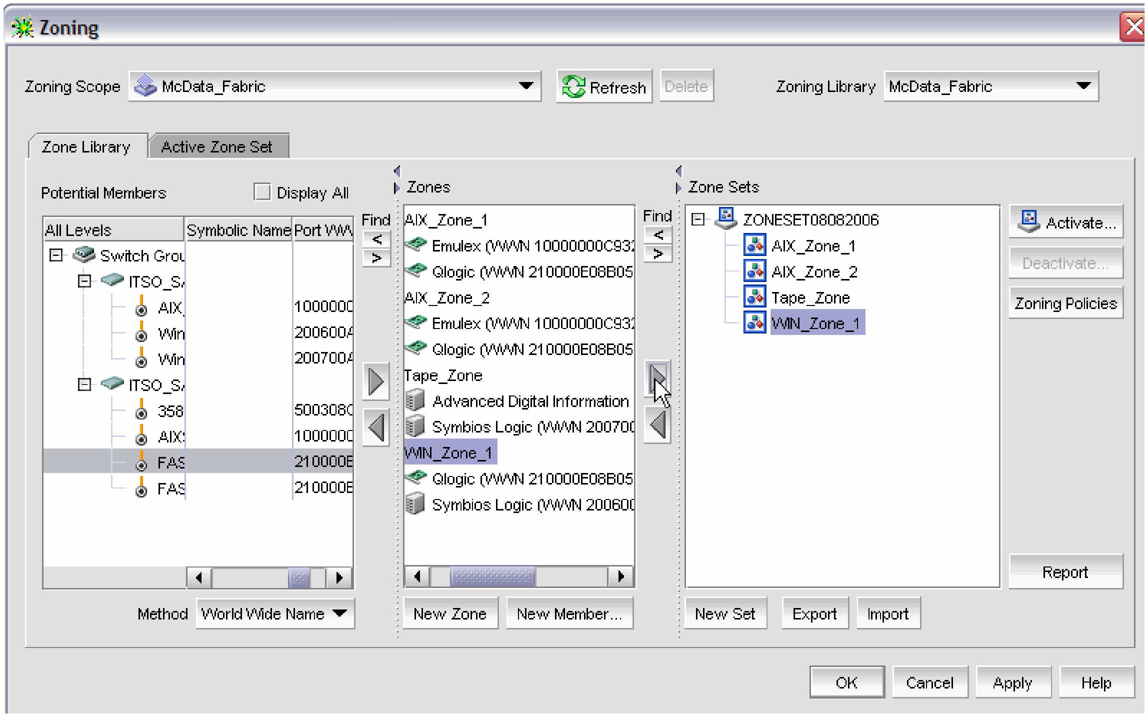
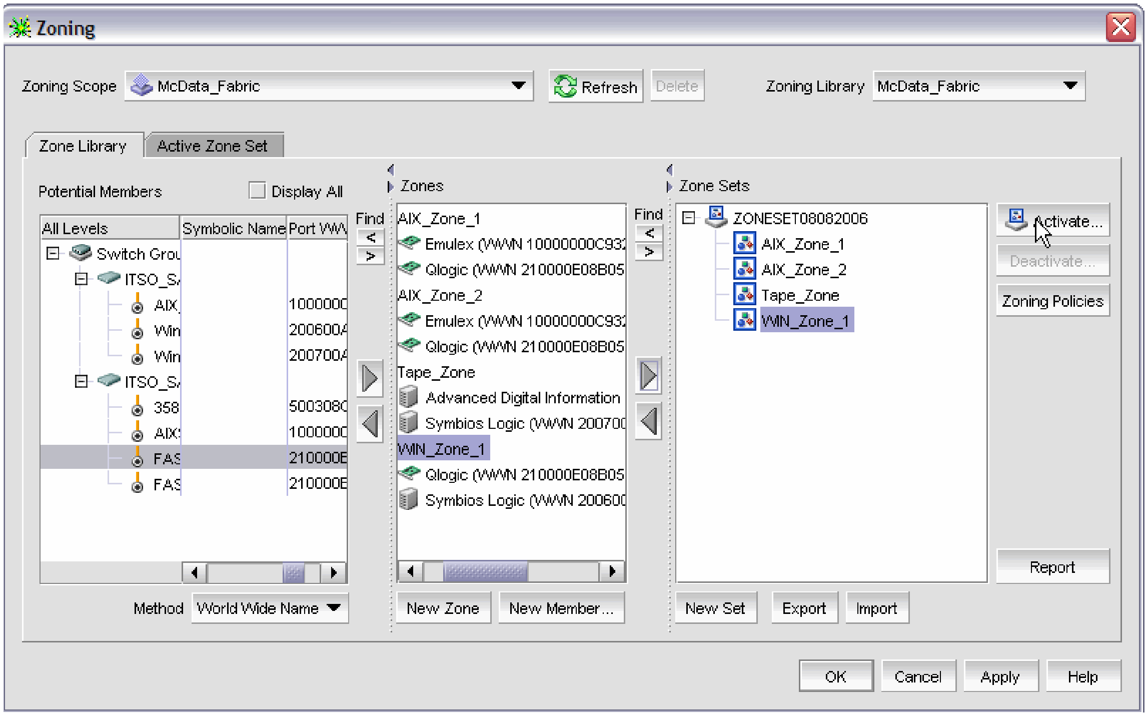

Zoning
Zoning Scope
McData_Fabric
Refresh
Delete
Zoning Library
McData_Fabric
Zone Library
Active Zone Set
Potential Members
Display All
All Levels
Symbolic Name
Port WW
Switch Grou
ITSO_S
AIX
Win
Win
ITSO_S
358
AIX
FAS
FAS
1000000
200600
200700
5003080
1000000
210000E
210000E
Find
<
>
Zones
AIX_Zone_1
Emulex (WWN 10000000C93
Qlogic (WWN 210000E08B05
AIX_Zone_2
Emulex (WWN 10000000C93
Qlogic (WWN 210000E08B05
Tape_Zone
Advanced Digital Information
Symbios Logic (WWN 200700
WIN_Zone_1
Qlogic (WWN 210000E08B05
Symbios Logic (WWN 200600
Zone Sets
ZONESET08082006
AIX_Zone_1
AIX_Zone_2
Tape_Zone
WIN_Zone_1
Activate...
Deactivate...
Zoning Policies
Report
Method
World Wide Name
New Zone
New Member...
New Set
Export
Import
OK
Cancel
Apply
Help

Figure 2-175 Zoning dialog window: Adding zones to a zone set

Activating the zone set and making the fabric zoned

To finish our zoning example, we now activate the zone set. This is done from the Zoning dialog window by highlighting the zone set and selecting the **Activate** button as shown in Figure 2-176.


Zoning Scope: McData_Fabric

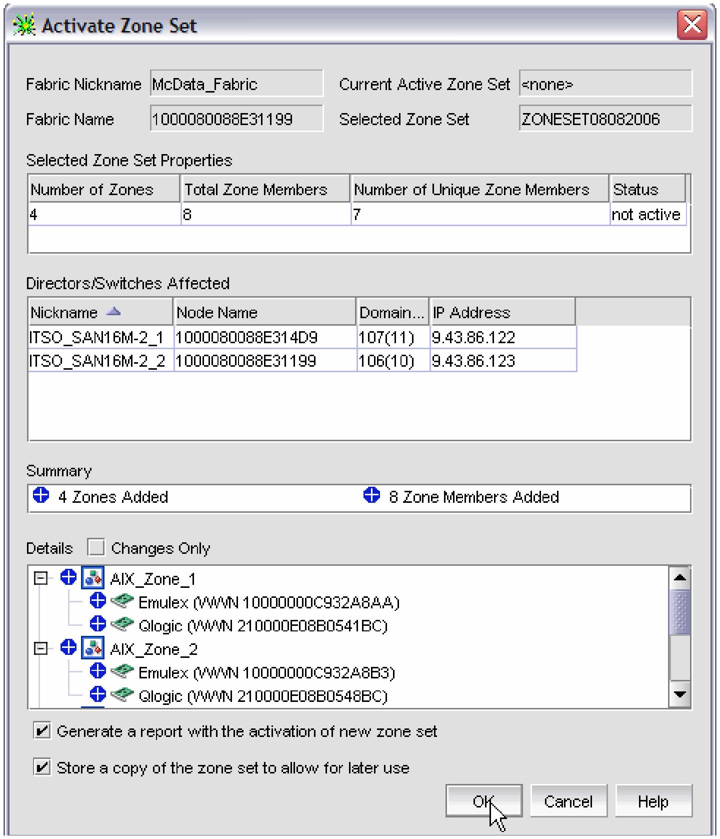
Zoning Library: McData_Fabric

Method: World Wide Name

Zoning
Refresh
Delete
Zone Library
Active Zone Set
Potential Members
Display All
All Levels
Symbolic Name
Port WW
Find
Switch Grou
ITSO_S
AIX_
Win
Win
ITSO_S
358
AIX
FAS
FAS
1000000
200600A
200700A
5003080
1000000
210000E
210000E
Zones
AIX_Zone_1
Emulex (WWN 10000000C93
Qlogic (WWN 210000E08B05
AIX_Zone_2
Emulex (WWN 10000000C93
Qlogic (WWN 210000E08B05
Tape_Zone
Advanced Digital Information
Symbios Logic (WWN 200700
WIN_Zone_1
Qlogic (WWN 210000E08B05
Symbios Logic (WWN 200600
New Zone
New Member...
Zone Sets
ZONESET08082006
AIX_Zone_1
AIX_Zone_2
Tape_Zone
WIN_Zone_1
Activate...
Deactivate...
Zoning Policies
Report
New Set
Export
Import
OK
Cancel
Apply
Help

Figure 2-176 Zone set activation

This action brings up a dialog box showing us the fabric name, current and new zone set, and the directors/switches affected, as illustrated in Figure 2-177.



Fabric Nickname McData_Fabric

Current Active Zone Set <none>

Fabric Name 1000080088E31199

Selected Zone Set ZONESET08082006

Selected Zone Set Properties

Number of Zones	Total Zone Members	Number of Unique Zone Members	Status
4	8	7	not active

Directors/Switches Affected

Nickname	Node Name	Domain...	IP Address
ITSO_SAN16M-2_1	1000080088E314D9	107(11)	9.43.86.122
ITSO_SAN16M-2_2	1000080088E31199	106(10)	9.43.86.123

Summary

- 4 Zones Added
- 8 Zone Members Added

Details ☐ Changes Only

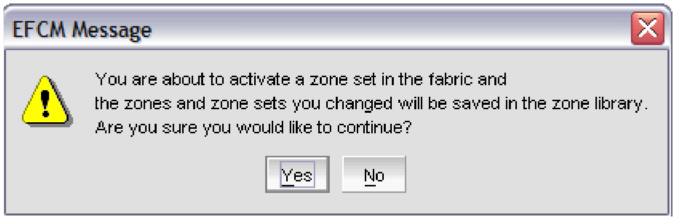
- AIX_Zone_1
  - Emulex (WWN 10000000C932A8AA)
  - Qlogic (WWN 210000E08B0541BC)
- AIX_Zone_2
  - Emulex (WWN 10000000C932A8B3)
  - Qlogic (WWN 210000E08B0548BC)

☑ Generate a report with the activation of new zone set

☑ Store a copy of the zone set to allow for later use

Figure 2-177 Zone set activation: Summary and detail

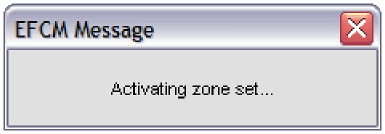
If we have modified an existing zone set and are activating the same zone set, we are presented with a window displaying the changes that are about to be made by the activation (Figure 2-178).


EFCM Message

You are about to activate a zone set in the fabric and
the zones and zone sets you changed will be saved in the zone library.
Are you sure you would like to continue?

Figure 2-178 Zone set activation: Confirmation

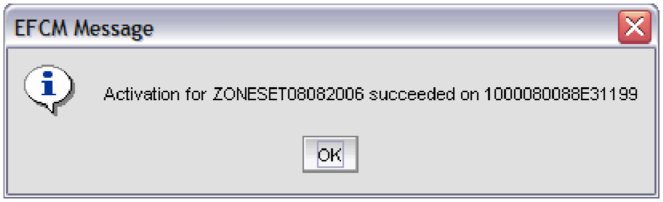
We confirm our changes and click **OK** (Figure 2-179).


EFCM Message

Activating zone set...

Figure 2-179 Zoneset activating

After the progress message shown in Figure 2-179, the activation complete frame is displayed as shown in Figure 2-180.click the **OK** tab to complete the activation.


EFCM Message

Activation for ZONESET08082006 succeeded on 1000080088E31199

Figure 2-180 Zoneset activation complete

Viewing the active zoning configuration

The icons of the active zone set and zones it contains now show up in colored icons, as opposed to non-active zones sets or zones (such as AIX_Zone_2 in this example), which appear with grayed out icons, as in Figure 2-181.

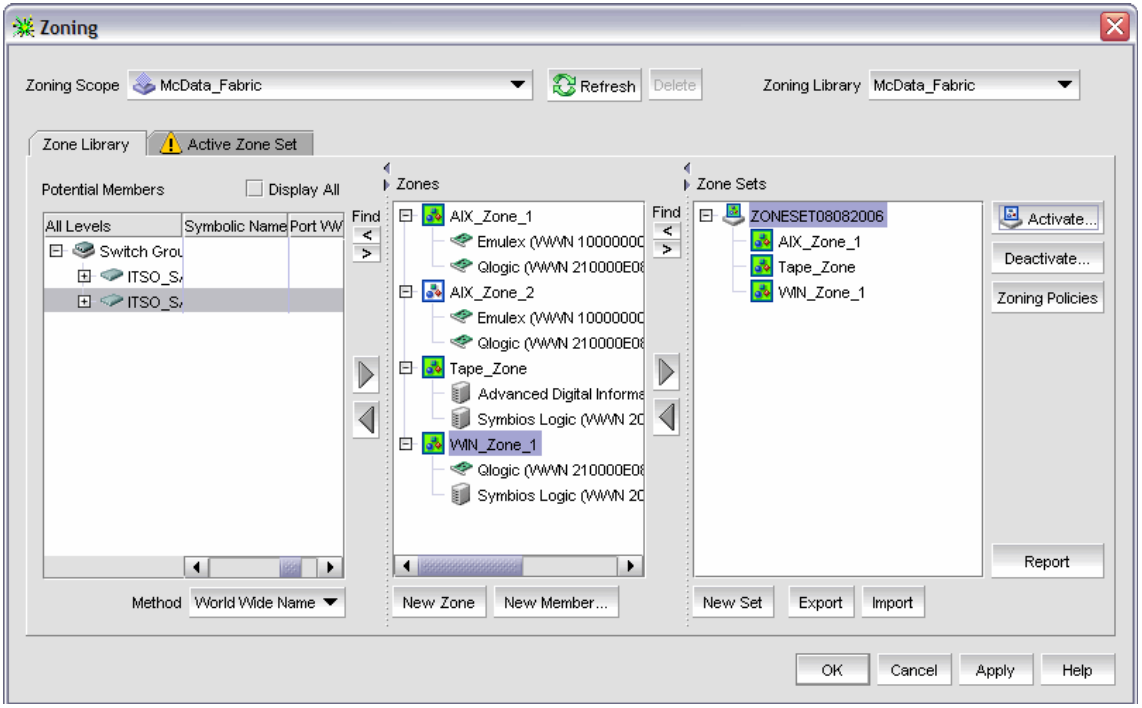

Zoning
Zoning Scope
McData_Fabric
Refresh
Delete
Zoning Library
McData_Fabric
Zone Library
Active Zone Set
Potential Members
Display All
All Levels
Symbolic Name
Port WW
Switch Grou
ITSO_S/
ITSO_S/
Find
<
>
Zones
AIX_Zone_1
Emulex (WWN 10000000
Qlogic (WWN 210000E0
AIX_Zone_2
Emulex (WWN 10000000
Qlogic (WWN 210000E0
Tape_Zone
Advanced Digital Informa
Symbios Logic (WWN 20
WIN_Zone_1
Qlogic (WWN 210000E0
Symbios Logic (WWN 20
Find
<
>
Zone Sets
ZONESET08082006
AIX_Zone_1
Tape_Zone
WIN_Zone_1
Activate...
Deactivate...
Zoning Policies
Report
Method
World Wide Name
New Zone
New Member...
New Set
Export
Import
OK
Cancel
Apply
Help

Figure 2-181 Zoning dialog window: Zone set activate

Modifying zone sets

We can also manipulate the zone sets by, for example, adding or removing zones, deactivating a zone set or saving the zone set. We can add a zone to the existing zone set with the same steps we used before.

For example, if we had a new AIX servers that we wanted to access our storage, we would first create a new zone and add the device members to that Zone, AIX_Zone_2, in our example. Then add them to the existing zone set. We could now select **Activate** to activate the zone set again, as shown in Figure 2-182.

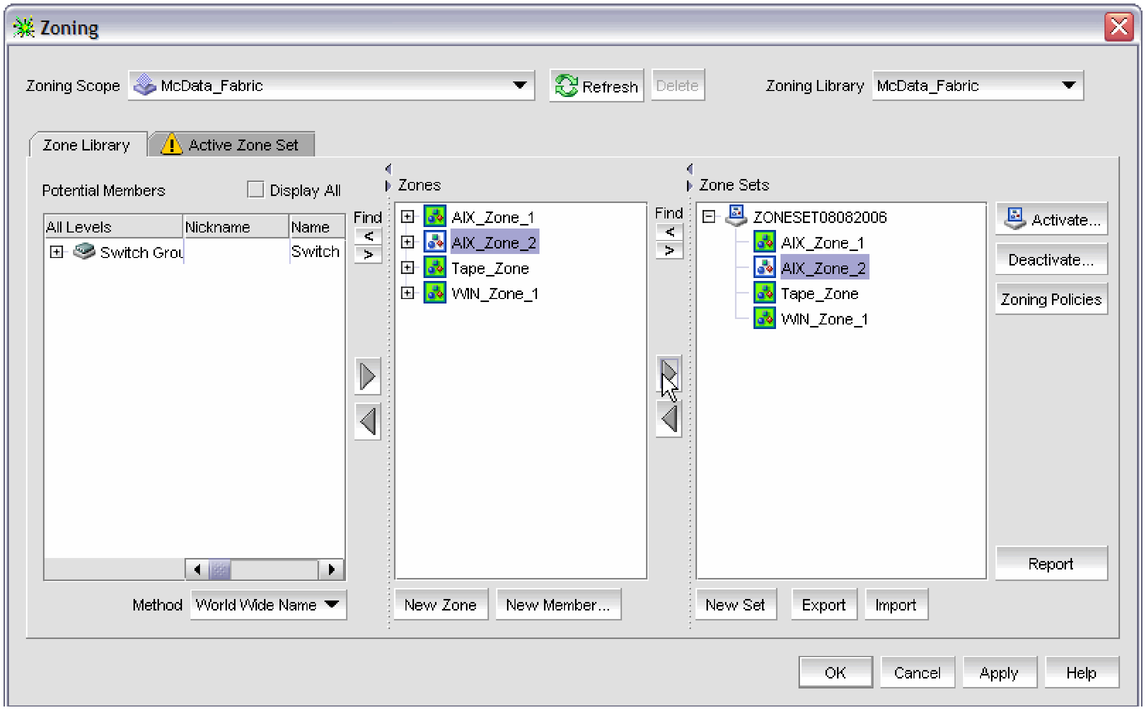
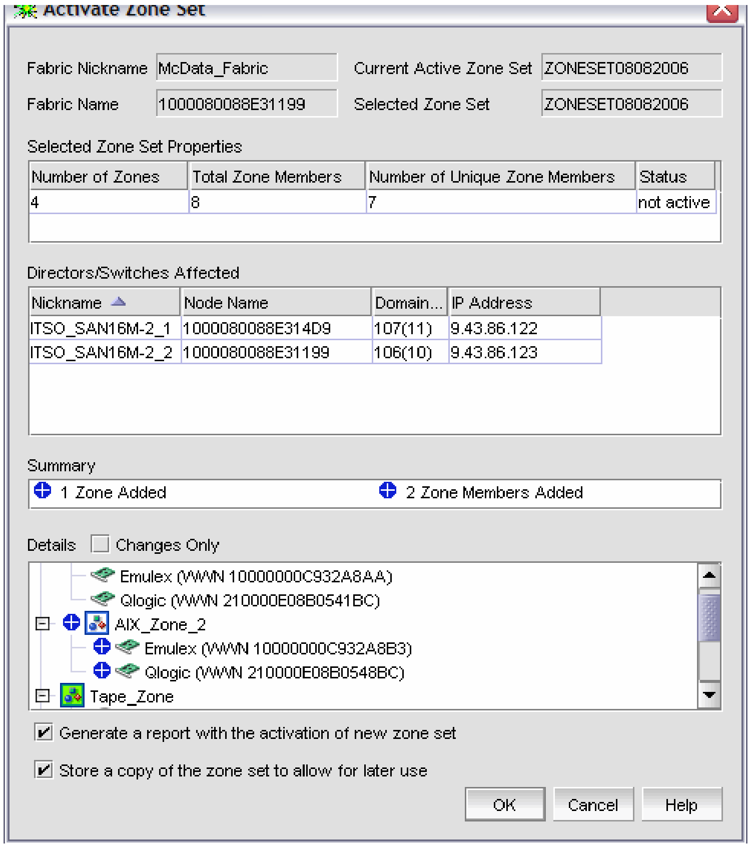

Zoning
Zoning Scope
McData_Fabric
Refresh
Delete
Zoning Library
McData_Fabric
Zone Library
Active Zone Set
Potential Members
Display All
All Levels
Nickname
Name
Switch Grou
Switch
Find
Method
World Wide Name
Zones
AIX_Zone_1
AIX_Zone_2
Tape_Zone
WIN_Zone_1
New Zone
New Member...
Zone Sets
ZONESET08082006
AIX_Zone_1
AIX_Zone_2
Tape_Zone
WIN_Zone_1
New Set
Export
Import
Activate...
Deactivate...
Zoning Policies
Report
OK
Cancel
Apply
Help

Figure 2-182 Adding a zone to existing zone set

This brings up a dialog box to display what changes are to be made; this is shown in Figure 2-183. Click the **OK** tab.



Fabric Nickname: McData_Fabric
Current Active Zone Set: ZONESET08082006
Fabric Name: 1000080088E31199
Selected Zone Set: ZONESET08082006

Selected Zone Set Properties

Number of Zones	Total Zone Members	Number of Unique Zone Members	Status
4	8	7	not active

Directors/Switches Affected

Nickname	Node Name	Domain...	IP Address
ITSO_SAN16M-2_1	1000080088E314D9	107(11)	9.43.86.122
ITSO_SAN16M-2_2	1000080088E31199	106(10)	9.43.86.123

Summary

1 Zone Added
2 Zone Members Added

Details ☐ Changes Only

```
    Emulex (WWN 10000000C932A8AA)
    Qlogic (WWN 210000E08B0541BC)
⊟ AIX_Zone_2
    Emulex (WWN 10000000C932A8B3)
    Qlogic (WWN 210000E08B0548BC)
⊟ Tape_Zone
```

☑ Generate a report with the activation of new zone set

☑ Store a copy of the zone set to allow for later use

Figure 2-183 Adding zone to existing zone set: Confirmation

If you want to create a new zoneset and activate, then the actions are the same as the previous steps. You would create a new zoneset and then add the zones you want to activate, as well as those in the old zoneset you want to keep. You would then activate the new zoneset as shown in Figure 2-184.

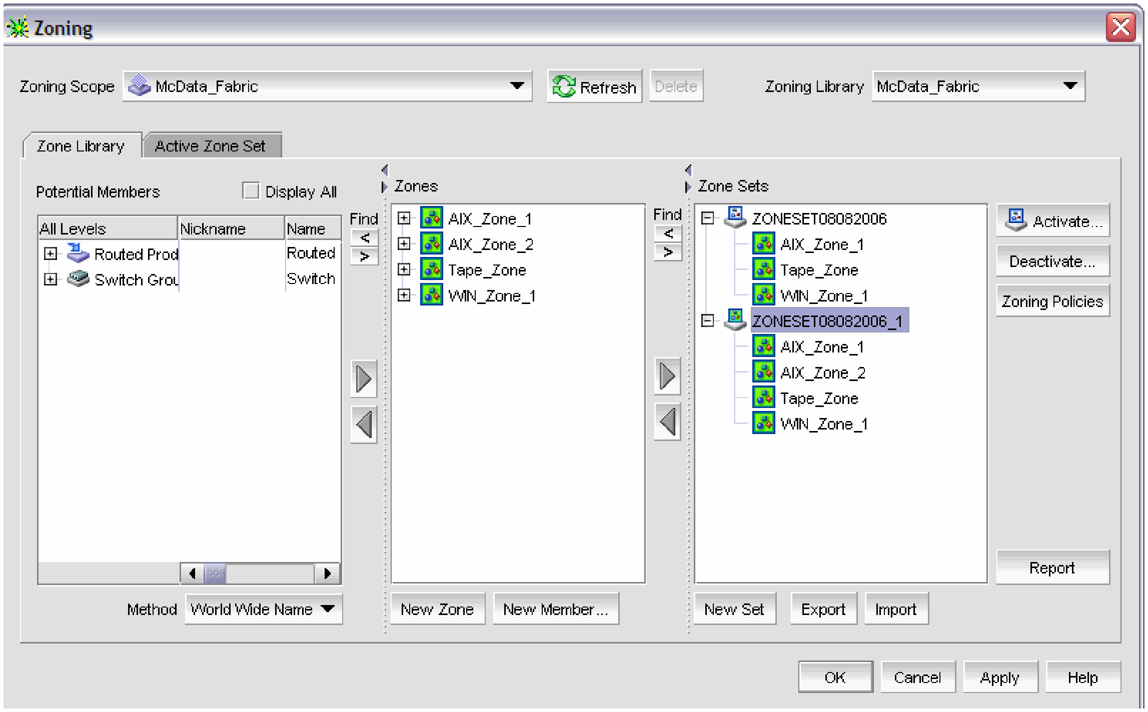
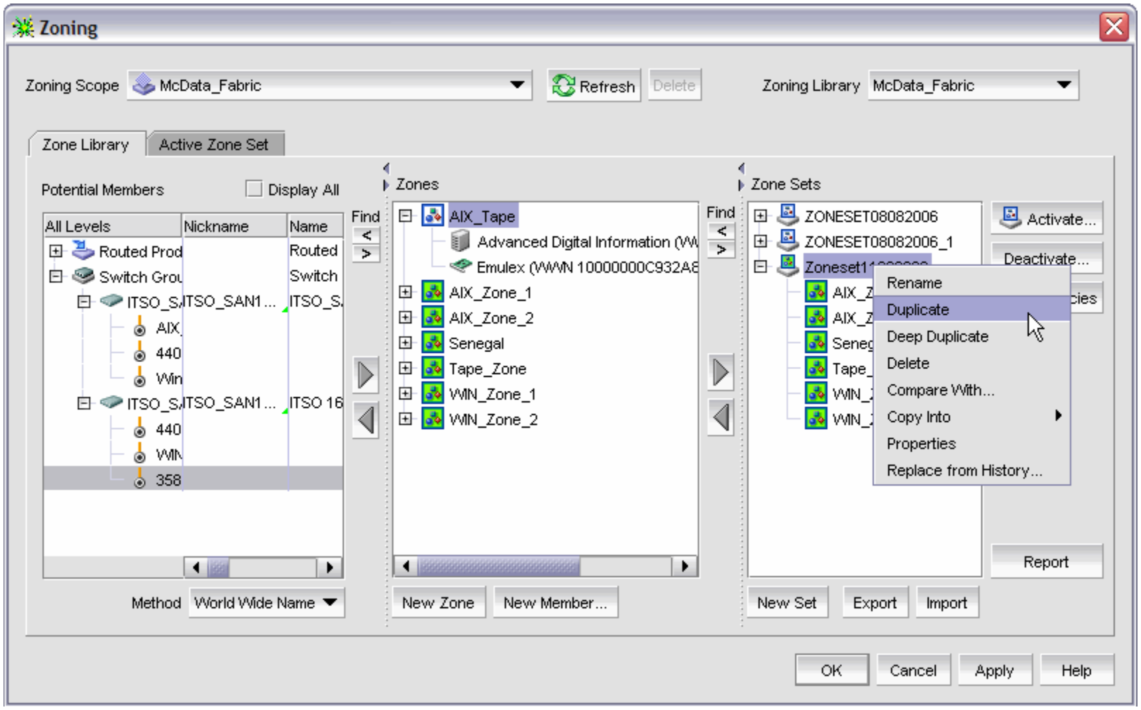

Zoning
Zoning Scope
McData_Fabric
Refresh
Delete
Zoning Library
McData_Fabric
Zone Library
Active Zone Set
Potential Members
Display All
All Levels
Nickname
Name
Routed Prod
Routed
Switch Grou
Switch
Find
Method
World Wide Name
Zones
AIX_Zone_1
AIX_Zone_2
Tape_Zone
WIN_Zone_1
New Zone
New Member...
Zone Sets
ZONESET08082006
AIX_Zone_1
Tape_Zone
WIN_Zone_1
ZONESET08082006_1
AIX_Zone_1
AIX_Zone_2
Tape_Zone
WIN_Zone_1
New Set
Export
Import
Activate...
Deactivate...
Zoning Policies
Report
OK
Cancel
Apply
Help

Figure 2-184 New zoneset activation

Zoneset duplication

We recommend that you should create a new zoneset for each change, as this ensures that you can back out to the previous good zoneset without having to make modifications to the active zoneset.

First add your zoning changes, AIX_Tape in our example, then using the right mouse button on the active zoneset, select **Duplicate**, as shown in Figure 2-185.



Zoning Scope: McData_Fabric

Zoning Library: McData_Fabric

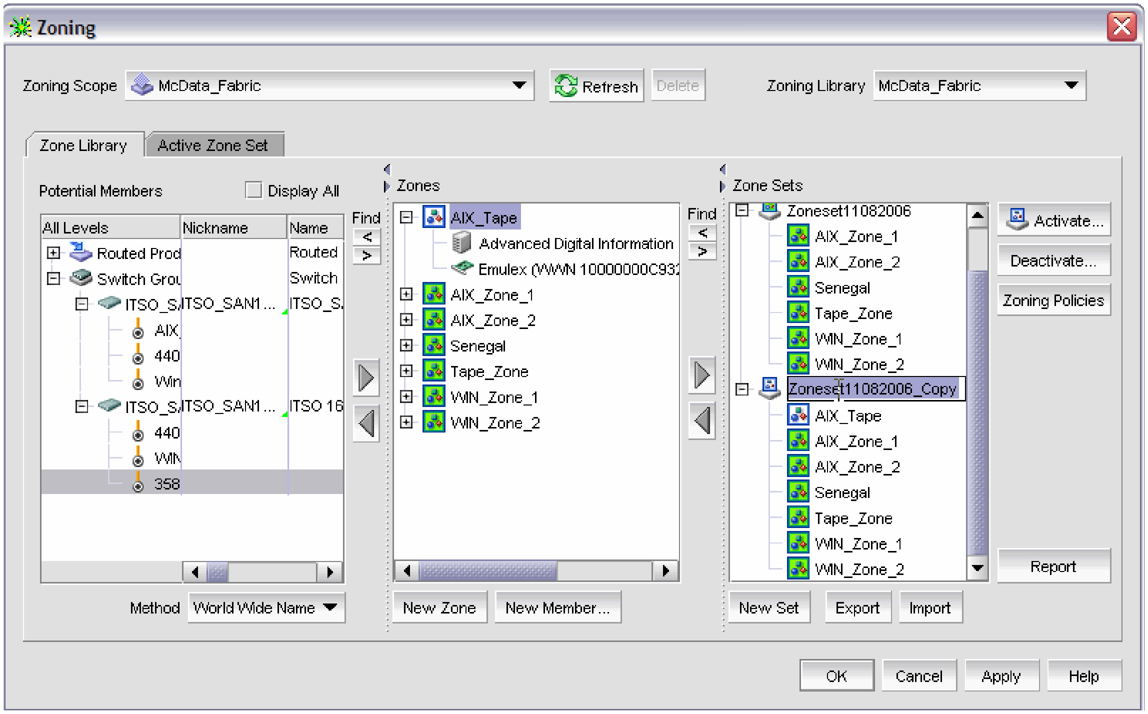
Method: World Wide Name

Zoning
Refresh
Delete
Zone Library
Active Zone Set
Potential Members
Display All
All Levels
Nickname
Name
Routed Prod
Routed
Switch Grou
Switch
ITSO_S/ITSO_SAN1...
ITSO_S.
AIX
440
Win
ITSO_S/ITSO_SAN1...
ITSO 16
440
WIN
358
Find
Zones
AIX_Tape
Advanced Digital Information (WW
Emulex (WWN 10000000C932A8
AIX_Zone_1
AIX_Zone_2
Senegal
Tape_Zone
WIN_Zone_1
WIN_Zone_2
New Zone
New Member...
Find
Zone Sets
ZONESET08082006
ZONESET08082006_1
Zoneset1
AIX_Z
AIX_Z
Seneg
Tape_
WIN_
WIN_
Rename
Duplicate
Deep Duplicate
Delete
Compare With...
Copy Into
Properties
Replace from History...
Activate...
Deactivate...
cies
Report
New Set
Export
Import
OK
Cancel
Apply
Help

Figure 2-185 Zoneset Duplication

This creates a duplicate zoneset of the Active ZoneSet and you can also use it to duplicate any other zoneset you might want to select.

You can now add the zoning changes to this exact duplicate of the active zoneset, as shown in Figure 2-186. When this is done, you can change the name of the duplicate zoneset to conform to your standards and activate this zoneset.


Zoning
Refresh
Delete
Zone Library
Active Zone Set
Potential Members
☐ Display All
All Levels
Nickname
Name
Routed Prod
Routed
Switch Grou
Switch
ITSO_S ITSO_SAN1...
ITSO_S
AIX
440
Win
ITSO_S ITSO_SAN1...
ITSO 16
440
WIN
358
Find
<
>
Zones
AIX_Tape
Advanced Digital Information
Emulex (WWN 10000000C93
AIX_Zone_1
AIX_Zone_2
Senegal
Tape_Zone
WIN_Zone_1
WIN_Zone_2
New Zone
New Member...
Zone Sets
Zoneset11082006
AIX_Zone_1
AIX_Zone_2
Senegal
Tape_Zone
WIN_Zone_1
WIN_Zone_2
Zoneset11082006_Copy
AIX_Tape
AIX_Zone_1
AIX_Zone_2
Senegal
Tape_Zone
WIN_Zone_1
WIN_Zone_2
Activate...
Deactivate...
Zoning Policies
Report
New Set
Export
Import
OK
Cancel
Apply
Help

Zoning Scope: McData_Fabric

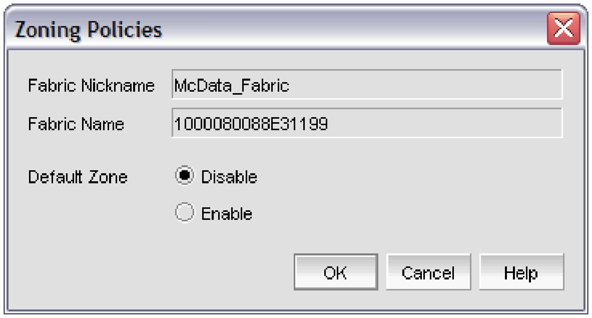
Zoning Library: McData_Fabric

Method: World Wide Name

Figure 2-186 Modifying duplicate zoneset

Default Zoning

We enable or disable the default zone via the **Zoning Policies** button as shown in Figure 2-184 on page 552, which spawns a dialog box with the options of **Disable** or **Enable**, as shown in Figure 2-187.


Zoning Policies
OK
Cancel
Help

Fabric Nickname: McData_Fabric

Fabric Name: 1000080088E31199

Default Zone: ● Disable ○ Enable

Figure 2-187 Default zone activation, confirmation

2.17 SANtegrity binding

SANtegrity binding enhances data security in large and complex SANs and consists of Fabric Binding and Switch Binding features. These features provide permit and deny operations for connecting a switch to the fabric, and end device attachment to the switch or fabric. SANtegrity, and therefore the binding features, can be enabled by purchasing a feature key and then installing and activating that feature key.

2.17.1 Fabric Binding

SANtegrity Fabric Binding gives access control tools across the fabric through which the system administrator can permit or deny switches from connecting to the fabric in a SAN. Without the Fabric Binding feature enabled, the fabric/zone configuration can be easily modified or deleted by connecting a new switch to the fabric, and there are no built-in mechanisms to permit or deny any switch from merging into the fabric. It gives greater control to the system administrator and gives protection from hacking into the fabric.

When Fabric Binding is activated, the Fabric Membership List (FML) automatically includes all the switches that are members of the fabric at the time of Fabric Binding activation. Switches and directors not in the Fabric Membership List at the time of activation are prohibited from joining, and raise alerts and attention indicators as invalid attachments.

In order to add a new switch to an existing fabric that has Fabric Binding activated, the existing Fabric Membership List must be updated with the WWN and domain ID of the switch or director that will be added to the fabric. The new switch or director must also have Fabric Binding activated (prior to joining the existing fabric) and a Fabric Membership List containing the WWN and domain ID of every switch in the existing fabric.

The list identifies switches by WWN and domain ID, so domain ID’s must be statically allocated while Fabric Binding is active. Because of this, the Insistent Domain ID feature is automatically enabled on each switch in the fabric when Fabric Binding is activated, and it cannot be disabled while Fabric Binding is active.

EFCM provides Fabric Binding configuration options in the Fabric Manager (that is to say, for a specific fabric), and not in the Element Manager. Fabric Binding can also be configured using the embedded CLI interface.

General rules for Fabric Binding

These are some general rules that apply to Fabric Binding:

- Not surprisingly, Fabric Binding activation is only available if SANtegrity Binding is installed.
- Fabric Binding activation is disallowed if the switch is offline. Switches can only be removed from the Fabric Membership List if they are not currently in the fabric.
- If the Fabric Binding configuration in the two fabrics is incompatible (that is to say, the Fabric Membership list is not identical), then the fabrics do not join. This is resolved by adding the attached switch to the Fabric Membership list or temporarily changing the Fabric Binding state to Inactive. The Fabric Membership list should be identical on all the switches in the fabric.
- Fabric Binding deactivation is prohibited if the Enterprise Fabric Mode is set to Active.

Configuring Fabric Binding

We use EFC Manager to demonstrate the procedure to configure Fabric Binding. From the EFC Manager, select the fabric on which the Fabric Binding feature has to be activated from the Fabric tree in the left-hand column, as shown in Figure 2-188.

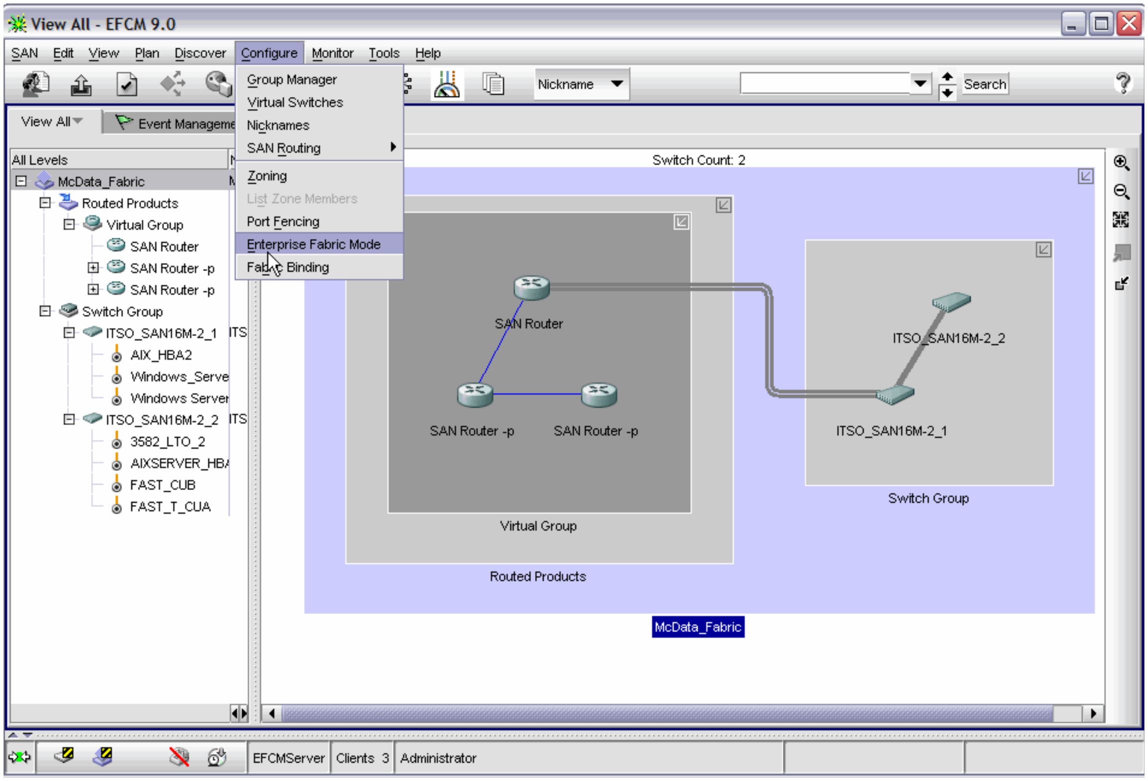
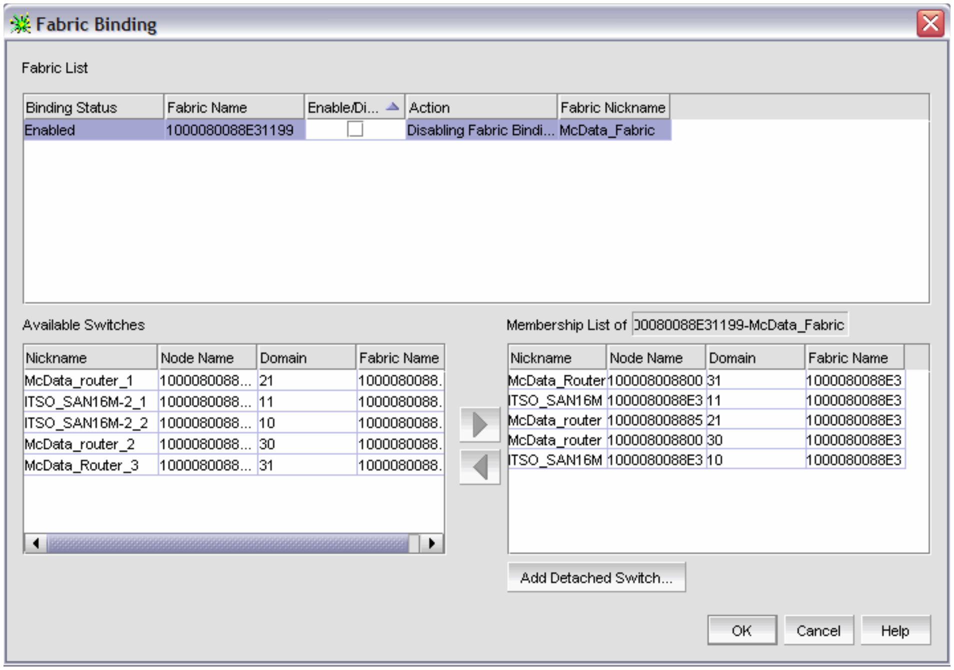

View All - EFCM 9.0
SAN
Edit
View
Plan
Discover
Configure
Monitor
Tools
Help
Group Manager
Virtual Switches
Nicknames
SAN Routing
Zoning
List Zone Members
Port Fencing
Enterprise Fabric Mode
Fabric Binding
Nickname
Search
View All
Event Manageme
All Levels
McData_Fabric
Routed Products
Virtual Group
SAN Router
SAN Router -p
SAN Router -p
Switch Group
ITSO_SAN16M-2_1
AIX_HBA2
Windows_Serve
Windows Server
ITSO_SAN16M-2_2
3582_LTO_2
AIXSERVER_HBA
FAST_CUB
FAST_T_CUA
Switch Count: 2
SAN Router
SAN Router -p
SAN Router -p
Virtual Group
Routed Products
ITSO_SAN16M-2_2
ITSO_SAN16M-2_1
Switch Group
McData_Fabric
EFCMServer
Clients 3
Administrator

Figure 2-188 Fabric tree list

The fabric nickname (McData_Fabric), once selected, topology view shows the number of switches in the fabric. Figure 2-188 shows that there are two switches and three routers in the fabric, so the Fabric Binding feature is activated on all these devices by default, and will automatically be included in the Fabric Membership List.

From the EFC Fabric Manager menu, select **Configure** → **Fabric Binding**.

The menu to enable Fabric Binding displays as shown in Figure 2-189.



Binding Status	Fabric Name	Enable/Di...	Action	Fabric Nickname
Enabled	1000080088E31199	☐	Disabling Fabric Bindi...	McData_Fabric

Nickname	Node Name	Domain	Fabric Name
McData_router_1	1000080088...	21	1000080088.
ITSO_SAN16M-2_1	1000080088...	11	1000080088.
ITSO_SAN16M-2_2	1000080088...	10	1000080088.
McData_router_2	1000080088...	30	1000080088.
McData_Router_3	1000080088...	31	1000080088.

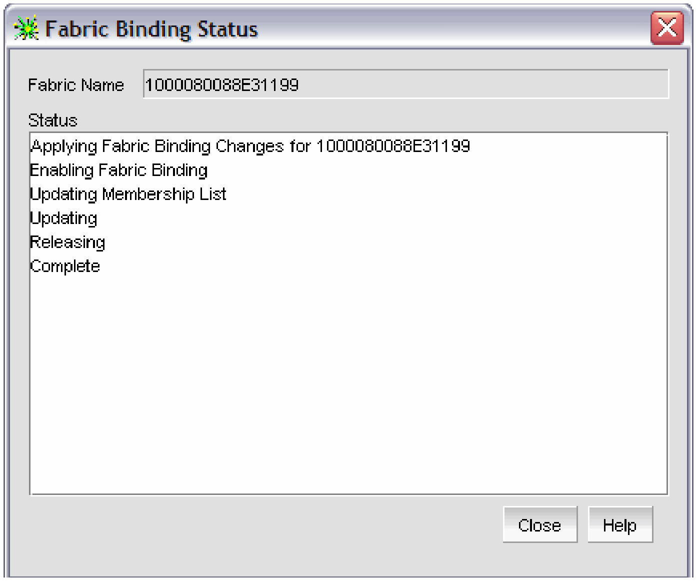
Membership List of 00080088E31199-McData_Fabric

Nickname	Node Name	Domain	Fabric Name
McData_Router	100008008800	31	1000080088E3
ITSO_SAN16M	1000080088E3	11	1000080088E3
McData_router	100008008885	21	1000080088E3
McData_router	100008008800	30	1000080088E3
ITSO_SAN16M	1000080088E3	10	1000080088E3

Figure 2-189 Configure Fabric Binding menu

Members (switches) can be added or removed from the list before Fabric Binding activation. It also allows you to add detached nodes to the list for future use. Check the **Enable/Disable** box and click the **OK** button.

During the activation process, you get a status display as shown in Figure 2-190.



Fabric Name 1000080088E31199

Status

Applying Fabric Binding Changes for 1000080088E31199
Enabling Fabric Binding
Updating Membership List
Updating
Releasing
Complete

Figure 2-190 Fabric Binding status window.

At this point the Fabric Binding feature has been activated and the fabric is now locked. Any new switch is denied access to join the fabric without manual intervention. The System Administrator must edit the Fabric Membership List and add the domain ID and WWN of the new switch to enable it to join the fabric.

Furthermore, the new switch must have SANtegrity installed, the Fabric Binding feature enabled, and also have the same Fabric Membership List currently active in the fabric.

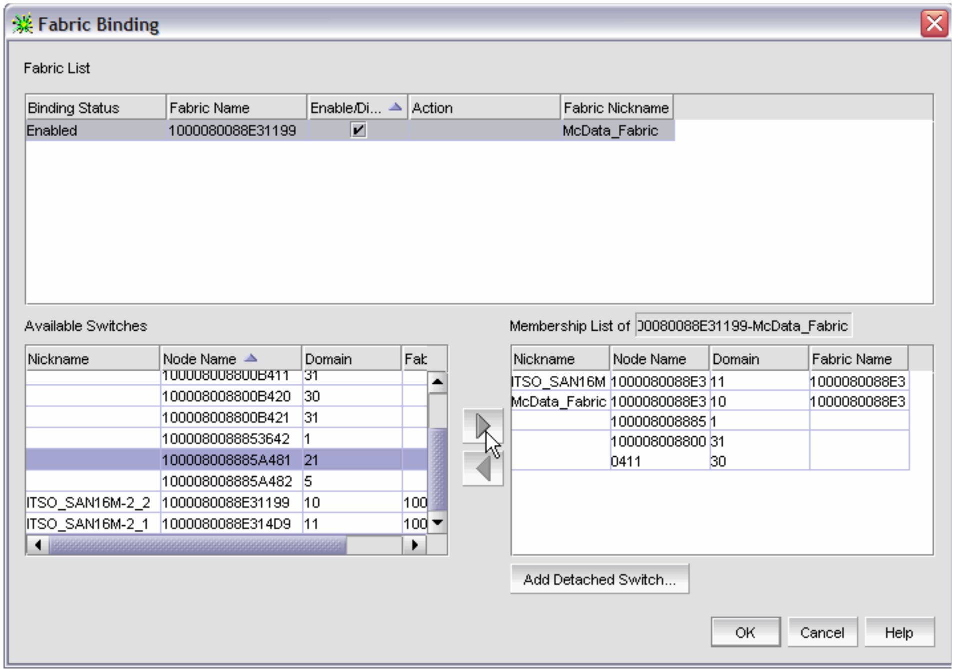
More details about SANtegrity can be found at this Web site:

`http://www.mcdata.com/knowcenter/techpubs/index.html`

Fabric Membership remove/add

To remove a member from Fabric Binding, this member must first be isolated from the fabric.

To add a new member (switch) to the list, from the EFC Manager, select **Configure** → **Fabric Binding**, then highlight the member to add and select the arrow as shown in Figure 2-191 and click **OK**.



Binding Status	Fabric Name	Enable/Di...	Action	Fabric Nickname
Enabled	1000080088E31199	☑		McData_Fabric

Nickname	Node Name	Domain	Fak
	100008008800B411	31	
	100008008800B420	30	
	100008008800B421	31	
	1000080088853642	1	
	100008008885A481	21	
	100008008885A482	5	
ITSO_SAN16M-2_2	1000080088E31199	10	100
ITSO_SAN16M-2_1	1000080088E314D9	11	100

Membership List of)0080088E31199-McData_Fabric

Nickname	Node Name	Domain	Fabric Name
ITSO_SAN16M	1000080088E3	11	1000080088E3
McData_Fabric	1000080088E3	10	1000080088E3
	100008008885	1	
	100008008800 0411	31 30	

Figure 2-191 Fabric Binding: Adding members

2.17.2 Switch Binding

SANtegrity Switch Binding allows an administrator the option to permit/deny which end devices can be connected to director or switch ports by specifying the WWN of the devices in the Switch Membership List. Without the Switch Binding feature active on the switch, any device can connect and, other than zoning, there is no built-in mechanism apart from Port Binding to prohibit end device connectivity. This feature provides an additional layer of security and greater access control tools for the system administrator managing complex environments that include a large number of devices.

When Switch Binding is enabled, only devices that are connected and online are identified and added to the Switch Membership List automatically. Thus the devices in the Switch Membership List are allowed to connect. Servers, storage, and other switches *not* in the Switch Membership List while Switch Binding is enabled, are prohibited from connecting, and raise alerts and attention indicators as invalid attachments.

Switch Binding enforcement modes

Switch Binding has several different enforcement modes, as we describe next.

Restrict E_Ports

E_Ports are blocked from forming ISL connections with any switch WWN not explicitly identified in the Switch Membership List. There is no restriction for F_Ports from connecting to the switch.

Restrict F_Ports

F_Ports prohibit connections from any end device not explicitly identified in the Switch Membership List. There is no restriction for E_Ports to form ISL connections with other switches.

Restrict All

Both E_Ports and F_Ports are prevented from connecting if the switch and end device WWN is not explicitly in the Switch Membership List.

Switch Binding rules

The following rules apply to the Switch Binding feature:

- The Switch Binding feature cannot be enabled if SANtegrity Binding is not installed.
- If the switch is online and Switch Binding is disabled, the switch automatically adds the WWN of currently connected/online devices to the Switch Membership List (SML) if they are not already in the list.
- If the switch is online and Switch Binding is already enabled, then the user is only allowed to change the enforcement mode (**Restrict E_Ports, Restrict F_Ports, *Restrict All)***. In this case, the switch must automatically add currently attached devices to the SML if any are not already in the list.

  If the switch is offline when Switch Binding is enabled, then the switch does not automatically add attached devices to the Switch Membership List.

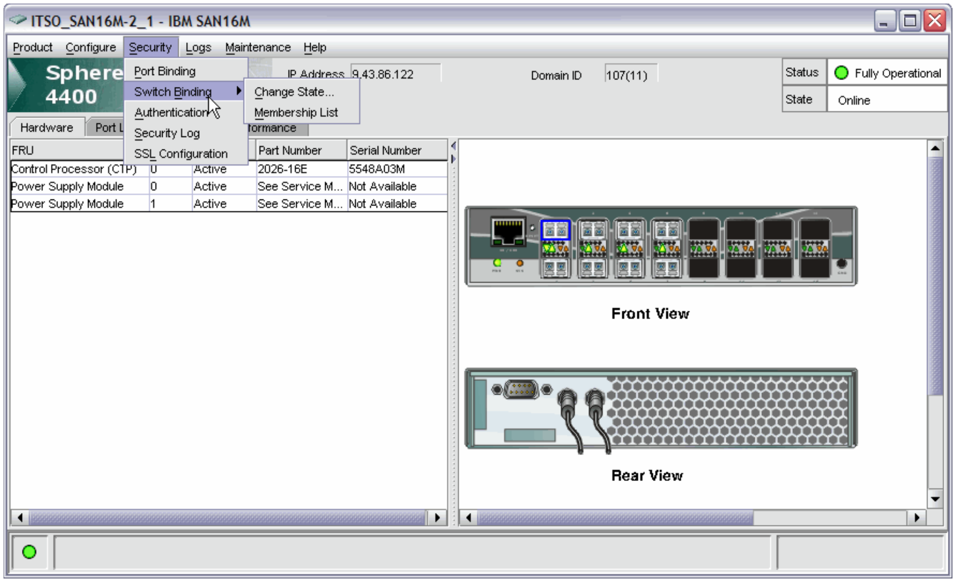
  WWNs can only be removed from the list if the switch is either offline, or Switch Binding is disabled, or if the WWN is not currently connected to the switch. A WWN can also be removed if Switch Binding is not enabled for the same port type as the WWN, meaning a WWN for an E_Port can be removed if Switch Binding is enabled and in Restrict F_Ports mode. If you try to remove a bound WWN, the following error message is displayed: `WWN is already connected on port number [N] and cannot be removed from the list. You must first block the port or disconnect the device.`

- If Switch Binding is enabled and restricting either E_Ports or All ports, then the switch searches for the WWN in the Switch Membership List. If the WWN is not in the list, an Invalid Attachment Reason Code is returned indicating a Switch Binding violation.
- If the WWN is not authorized, the port is placed in the **Invalid Attachment** state, and an Event Log entry (WWN Not Authorized) is generated. This is resolved in several different ways, such as adding the attached switch to the Switch Membership List, changing the Switch Binding state from Restricting E_Ports to Restricting F_Ports, or changing the Switch Binding state to Disabled.
- When a new device attempts to login to the fabric, the switch determines if the Port WWN of the attached device is authorized to connect in the following order:
- The WWN is verified against the current Port Binding configuration.
- The WWN is verified against the current Switch Binding configuration.
- If Switch Binding is enabled and restricting either F_Ports or All ports, then the switch searches for the WWN in the Switch Membership List. If the WWN is not in the list, the switch returns an Invalid Attachment Reason Code indicating a Switch Binding violation. If the WWN is not authorized, the port is placed in the Invalid Attachment state, and an Event Log entry (WWN Not Authorized) is generated.
- Switch Binding Disablement is prohibited if Enterprise Fabric Mode is Active and the switch is online. User interfaces display an error message.

Configuring Switch Binding

Switch Binding is configured independently on each switch. Before the Switch Binding feature is enabled, it is best to verify the Switch Membership List to ensure that all the devices are attached to the Switch, and you can permit or deny any device from the Edit Membership List menu.

From the EFCM Element Manager menu, select **Security** → **Switch Binding** → **Membership List...** as shown in Figure 2-192.


ITSO_SAN16M-2_1 - IBM SAN16M
Product
Configure
Security
Logs
Maintenance
Help
Sphere 4400
Port Binding
Switch Binding
Authentication
Security Log
SSL Configuration
Change State...
Membership List
Hardware
Port L
formance
Front View
Rear View

IP Address 9.43.86.122

Domain ID 107(11)

Status Fully Operational

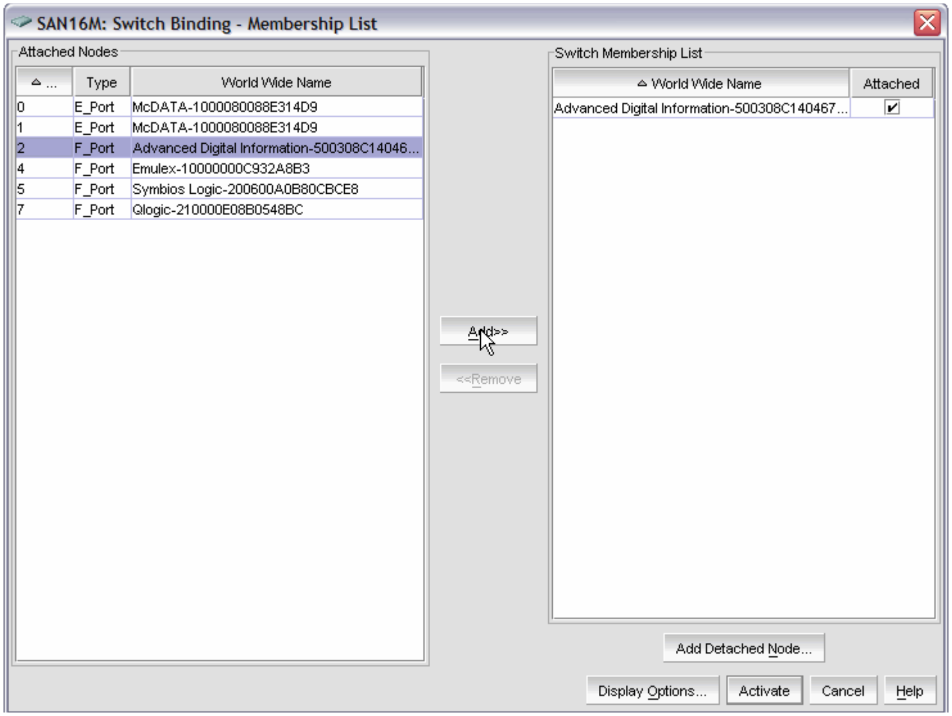
State Online

FRU			Part Number	Serial Number
Control Processor (CTP)	0	Active	2026-16E	5548A03M
Power Supply Module	0	Active	See Service M...	Not Available
Power Supply Module	1	Active	See Service M...	Not Available

Figure 2-192 Configure Switch Binding, Edit Membership List

The Edit Membership List menu is displayed. It lists all the end devices that are currently connected/online to the switch as shown in Figure 2-193.

From here you can add and remove members from the Switch Membership List. To add a device that is currently attached but not in the Switch Membership List, select the WWN of the device under the Attached Nodes list and it enables the **Add>>** button, which you can then click, as shown in Figure 2-193.


SAN16M: Switch Binding - Membership List
Attached Nodes
Switch Membership List
Add>>
<<Remove
Add Detached Node...
Display Options...
Activate
Cancel
Help

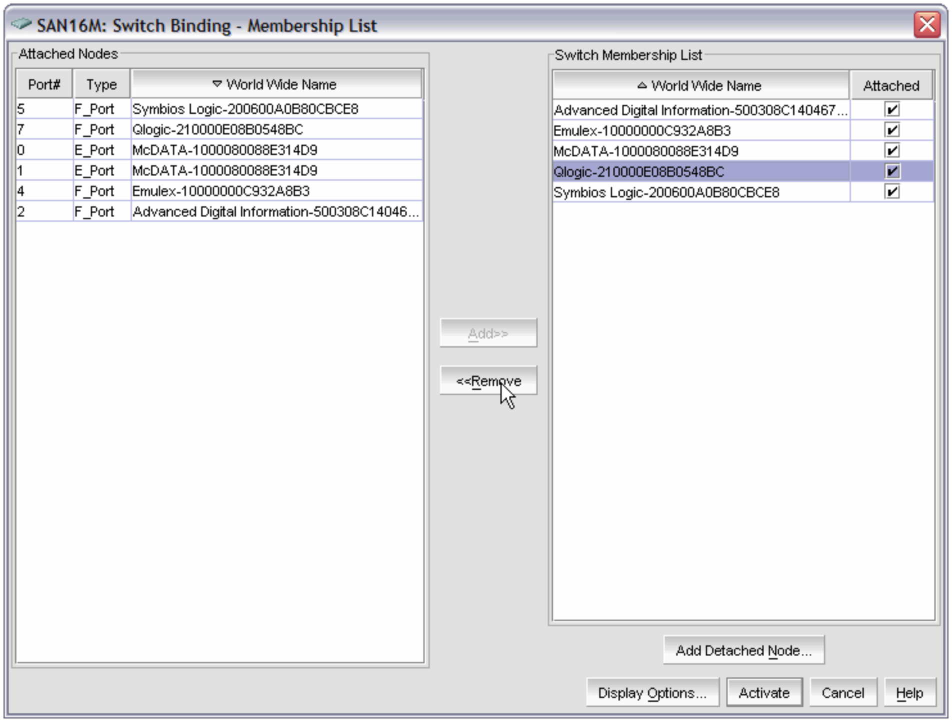
...	Type	World Wide Name
0	E_Port	McDATA-1000080088E314D9
1	E_Port	McDATA-1000080088E314D9
2	F_Port	Advanced Digital Information-500308C14046...
4	F_Port	Emulex-10000000C932A8B3
5	F_Port	Symbios Logic-200600A0B80CBCE8
7	F_Port	Qlogic-210000E08B0548BC

World Wide Name	Attached
Advanced Digital Information-500308C140467...	☑

Figure 2-193 Switch Binding, Edit Membership List, Add

Attention: The Switch Membership List can be edited only if the Switch Binding feature is disabled.

Similarly, the end devices can be removed from the Switch Membership List by selecting the device under the Switch Membership List, as it enables the **<<Remove** option button, as shown in Figure 2-194.


SAN16M: Switch Binding - Membership List
Attached Nodes
Switch Membership List
Add>>
<<Remove
Add Detached Node...
Display Options...
Activate
Cancel
Help

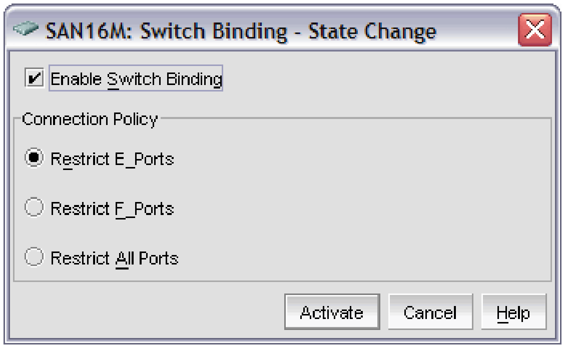
Port#	Type	World Wide Name
5	F_Port	Symbios Logic-200600A0B80CBCE8
7	F_Port	Qlogic-210000E08B0548BC
0	E_Port	McDATA-1000080088E314D9
1	E_Port	McDATA-1000080088E314D9
4	F_Port	Emulex-10000000C932A8B3
2	F_Port	Advanced Digital Information-500308C14046...

World Wide Name	Attached
Advanced Digital Information-500308C140467...	☑
Emulex-10000000C932A8B3	☑
McDATA-1000080088E314D9	☑
Qlogic-210000E08B0548BC	☑
Symbios Logic-200600A0B80CBCE8	☑

Figure 2-194 Switch Binding, Edit Membership List, Remove

The Switch Binding Change State and the enforcement mode configuration options are available from the EFCM Element Manager view by selecting **Security** → **Switch Binding** → **Change State...** as shown in Figure 2-192 on page 563.

From the Switch Binding Change State menu, check the **Enable Switch Binding** option, and by default the **Restrict E Ports** option is selected as shown in Figure 2-195. Select the port type or all ports from the selection buttons.



☑ Enable Switch Binding

Connection Policy

● Restrict E_Ports

○ Restrict F_Ports

○ Restrict All Ports

Figure 2-195 Switch Binding, Change State

When Switch Binding is enabled, the option to edit Switch Membership List is not available, but it allows you to change the enforcement mode.

2.17.3 Port Binding

When port binding is enabled, only a specific device can communicate through the port. This device is specified by the WWN or nickname entered into the Bound WWN field (either the Attached WWN or Detached WWN options). With the check box cleared, any device can communicate through the port even if a WWN or nickname is specified in the Bound WWN field.

Port Binding is a standard feature, and as such does not require the SANtegrity Binding feature to be licensed. It is enabled at the individual port level, and provides a way to restrict attachment to that port to a specific WWN.

One way to set up port binding is directly from the Element Manager Hardware view, right-click a the port selected and select Port Binding from the pop-up menu. If the **Port Binding** check box is not checked, then any WWN can connect. See Figure 2-196.

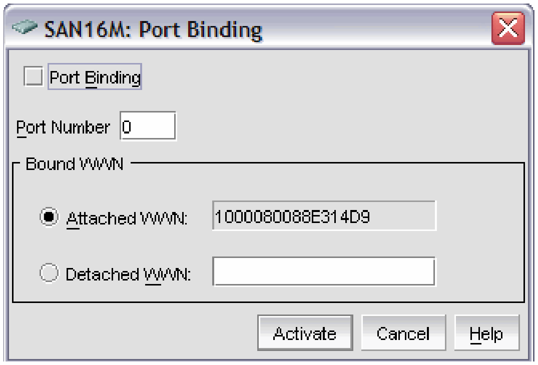

SAN16M: Port Binding
☐ Port Binding
Port Number 0
Bound WWN
● Attached WWN: 1000080088E314D9
○ Detached WWN:
Activate
Cancel
Help

Figure 2-196 Port binding

You can also configure port binding the EFCM Element Manager view by selecting **Security** → **Switch Binding** from the Configure Ports window, and from the **Configure** → **Ports** window.

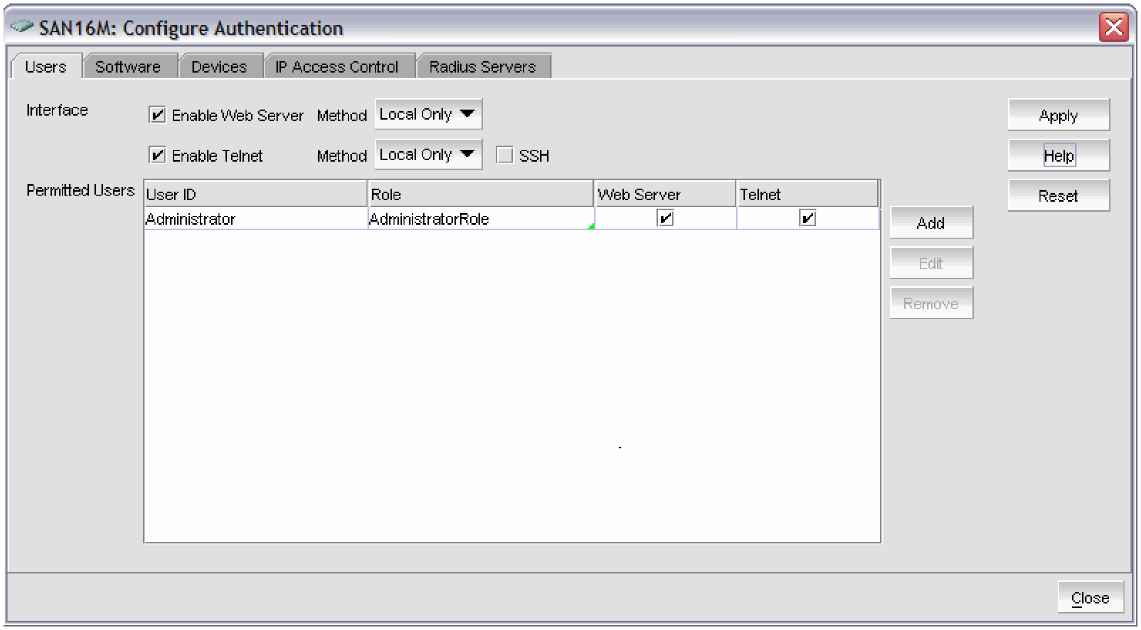
2.18 SANtegrity Authentication

If licensed, selecting **Security** → **Authentication** opens a multi-tab window. This provides a central place to manage access to the switch via the various interfaces, and the types of security to use.

> **Important:** If you enable any security features, make sure that you record all of this information and keep a copy of it in a secure location.

Users tab

From this tab, shown in Figure 2-197, you can enable or disable the EFCM Basic (EFCM Web Server), and Telnet interfaces. You can also select the method of authentication to be used for each, restrict access by user ID to these interfaces, and enable SSH.


SAN16M: Configure Authentication
Users
Software
Devices
IP Access Control
Radius Servers
Apply
Help
Reset
Add
Edit
Remove
Close

Interface

☑ Enable Web Server Method Local Only

☑ Enable Telnet Method Local Only ☐ SSH

Permitted Users

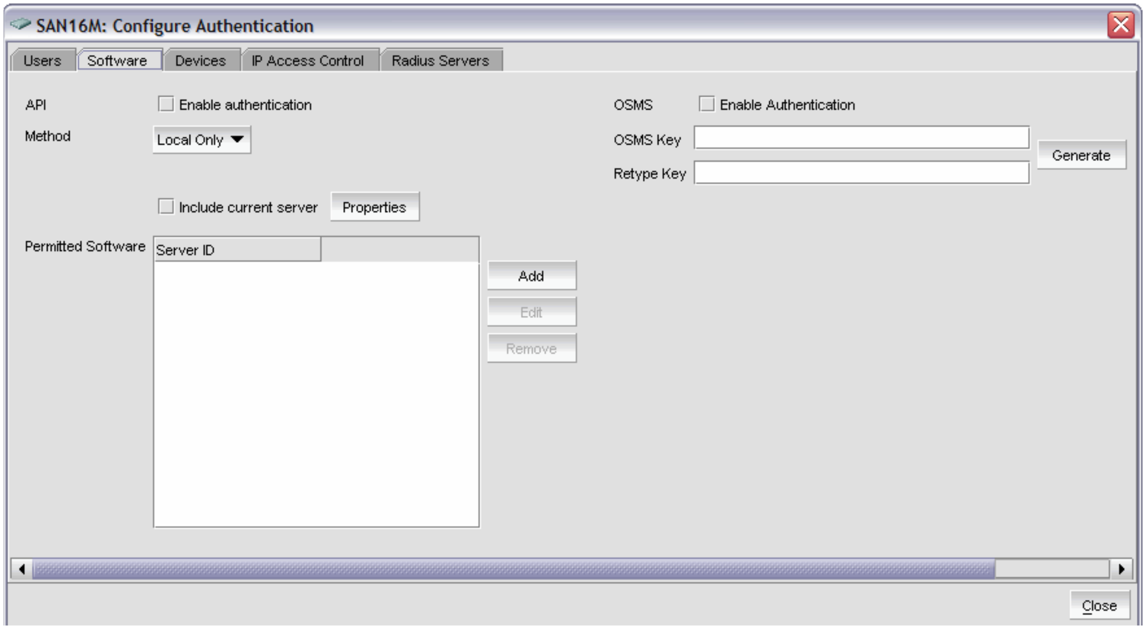
User ID	Role	Web Server	Telnet
Administrator	AdministratorRole	☑	☑

Figure 2-197 SANtegrity Authentication, Users tab

Software tab

This tab, shown in Figure 2-198, allows the Security Administrator to define software access to the switch or director through API and OSMS interfaces. Unlike the Web server and Telnet interfaces, the API and OSMS authentication require a CHAP secret as password.

The OSMS interface is for software to manage the switch or director in-band over Fibre Channel. The only information required for the OSMS interface is the OSMS secret. API users are identified by their designated software ID. Typically, the API user is the current SAN Management server, and its name is the server name defined at installation. Whenever the current server is present in the Permitted Software list, the Software tab displays with an asterisk next to the current server ID. If the API authentication is enabled, then ensure that the management server is included as a permitted server.



API ☐ Enable authentication

Method: Local Only

☐ Include current server

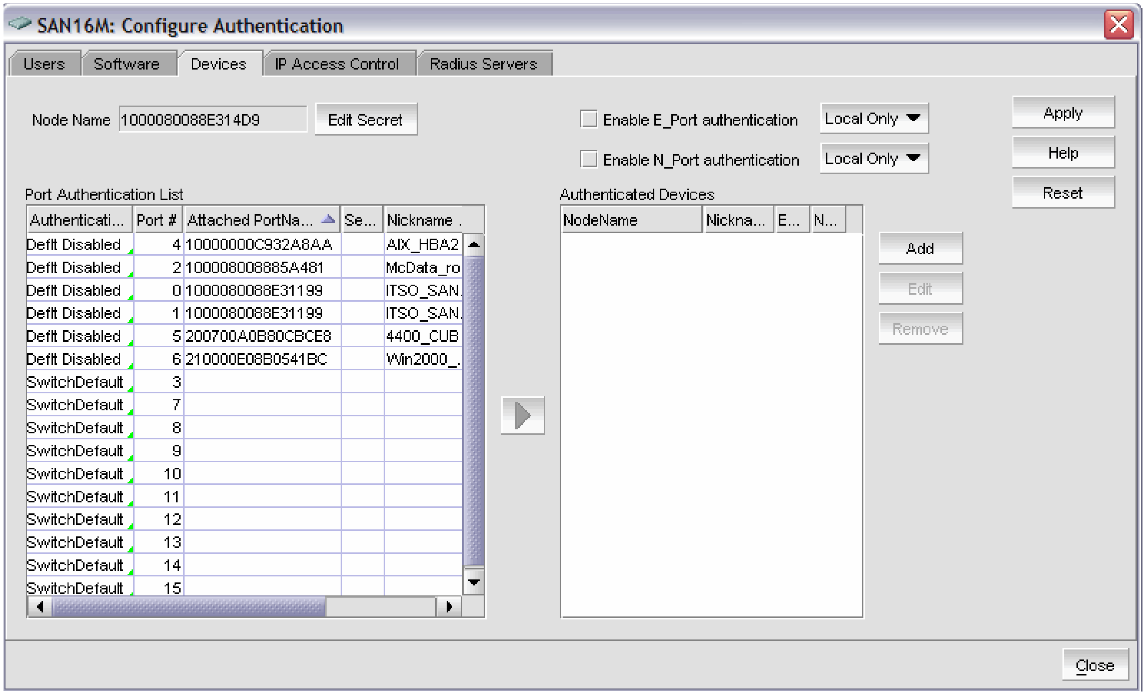
OSMS ☐ Enable Authentication

SAN16M: Configure Authentication
Users
Software
Devices
IP Access Control
Radius Servers
OSMS Key
Retype Key
Generate
Properties
Permitted Software
Server ID
Add
Edit
Remove
Close

Figure 2-198 SANtegrity Authentication, Software tab

Devices

The Devices tab, shown in Figure 2-199, defines whether the switch or director requires the other switch or director to authenticate, before connection into the existing switch is allowed. Device authentication is configured on a port-by-port basis. You can specify default authentication settings for the switch or director; and you can also configure individual switch and director ports to always authenticate or to never authenticate.



Node Name 1000080088E314D9

☐ Enable E_Port authentication Local Only

☐ Enable N_Port authentication Local Only

Port Authentication List

Authenticati...	Port #	Attached PortNa...	Se...	Nickname .
Deflt Disabled	4	10000000C932A8AA		AIX_HBA2
Deflt Disabled	2	100008008885A481		McData_ro
Deflt Disabled	0	1000080088E31199		ITSO_SAN.
Deflt Disabled	1	1000080088E31199		ITSO_SAN.
Deflt Disabled	5	200700A0B80CBCE8		4400_CUB
Deflt Disabled	6	210000E08B0541BC		Win2000_.
SwitchDefault	3			
SwitchDefault	7			
SwitchDefault	8			
SwitchDefault	9			
SwitchDefault	10			
SwitchDefault	11			
SwitchDefault	12			
SwitchDefault	13			
SwitchDefault	14			
SwitchDefault	15			

Authenticated Devices

NodeName	Nickna...	E...	N...

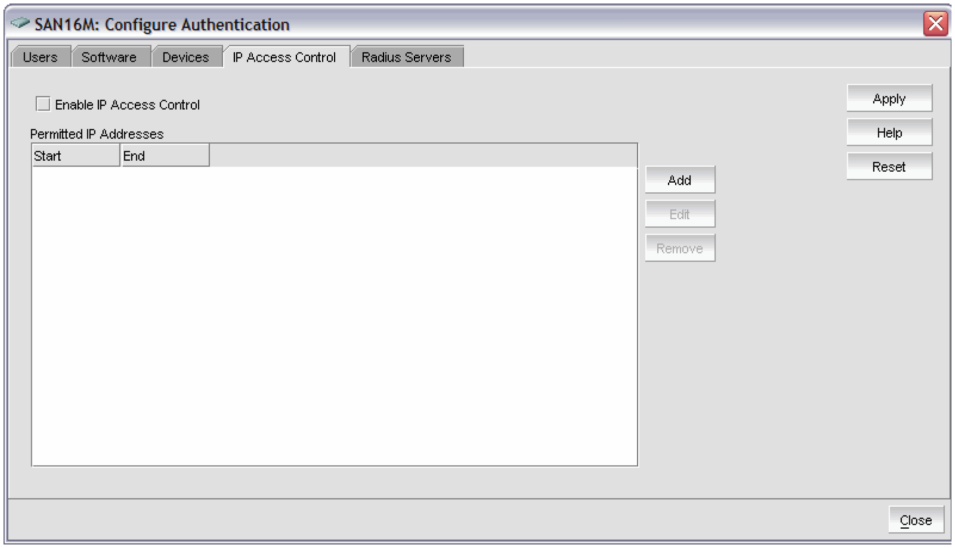
Figure 2-199 SANtegrity Authentication, Devices tab

You can also use the Devices tab to define the devices that are allowed to connect to authenticating ports. The features in the Devices tab can only be configured if the switch has the proper Product Feature Enablement key installed. If not, the Devices tab is disabled.

Note: Port authentication settings override switch authentication settings.

IP Access Control

This tab, shown in Figure 2-200, lets you restrict the IP addresses that are allowed to manage the switch. If the IP Access Control (IP ACL) feature is enabled, IP addresses that are not on this list cannot manage the switch or director.


SAN16M: Configure Authentication
Users
Software
Devices
IP Access Control
Radius Servers
Apply
Help
Reset
Add
Edit
Remove
Close

☐ Enable IP Access Control

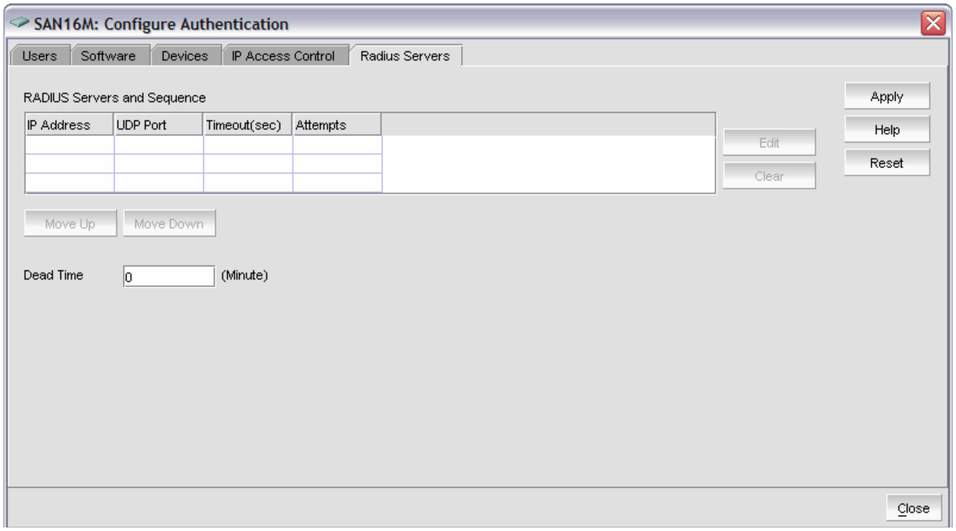
Permitted IP Addresses

Start	End

Figure 2-200 SANtegrity Authentication, IP Access Control tab

Radius Servers

Use this tab, shown in Figure 2-201, to specify the RADIUS servers from which the switch or director obtains authentication information. Use of the tab is optional. It is only necessary if the switch or director is using RADIUS authentication.


SAN16M: Configure Authentication
Users
Software
Devices
IP Access Control
Radius Servers
RADIUS Servers and Sequence
IP Address
UDP Port
Timeout(sec)
Attempts
Edit
Clear
Apply
Help
Reset
Move Up
Move Down
Close

Dead Time 0 (Minute)

Figure 2-201 SANtegrity Authentication, Radius Servers tab

Refer to the relevant product's *Element Manager User Manual* for detailed information on enabling the various security features.

2.19 Multiple switch environment

The design of a multiple switch fabric is outside of the scope of this book. What we cover in this section are the technologies used to build multiple switch fabrics.

McDATA support 24 switches/directors in a single fabric, and a maximum of three hops in a route (a hop is a switch-to-switch link, or ISL).

> **Note:** In IP networking, a hop count means the number of connectivity devices (for instance, routers) between the source and destination. This makes up the difference of one more hop in IP networking than in FC networks with the same amount of interconnected devices.

2.19.1 Inter-Switch Link

The basic technology for joining switches together is the Inter-Switch Link (ISL), which is the connection of an E_Port on one switch to an E_Port on another switch.

For performance and redundancy reasons, it is normal to have a minimum of two ISLs between any two switches, and for high bandwidth and larger fabric environments it might be necessary to have several more.

Remember that every switch port that is used for an ISL, is one less available for a device connection. As such, you should consider using higher port-count switches if you expect to grow beyond a small fabric.

For example, joining four 16 port switches with two ISLs between every switch (as shown in Figure 2-202) uses 24 of the total 64 ports as E_Ports, whereas joining two 32 port switches with four ISLs, only uses eight of the total 64 ports as E_Ports.

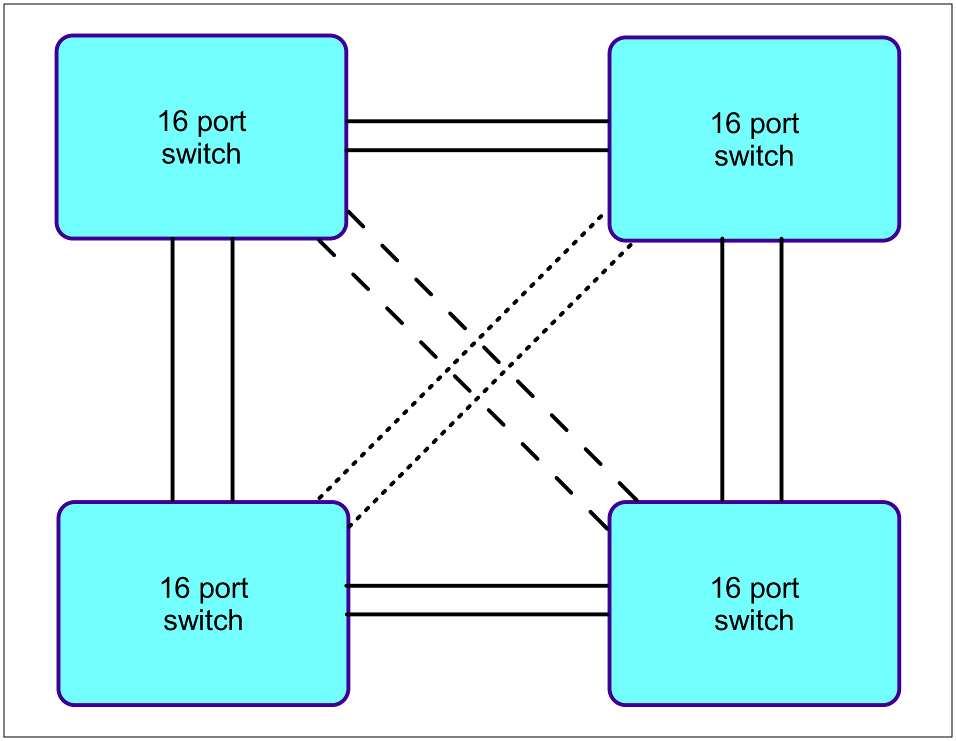


Figure 2-202 ISLs for four small switches

The same principle applies to larger port count devices, such as directors. Using directors would have the additional advantage that you could start with only 64 ports in the director, and grow the port count by adding more cards to the existing directors. You would also gain from the additional availability characteristics of a director.

2.19.2 Preferred pathing

As stated in “Preferred Path” on page 391, it is possible to influence the choice of ISLs used for routing frames across multiple switches.

The dotted blue line in Figure 2-203 shows the preferred route of the first hop for host traffic entering on port 10 between switch 1 and switch 2 when targeting Disk A on switch 3.

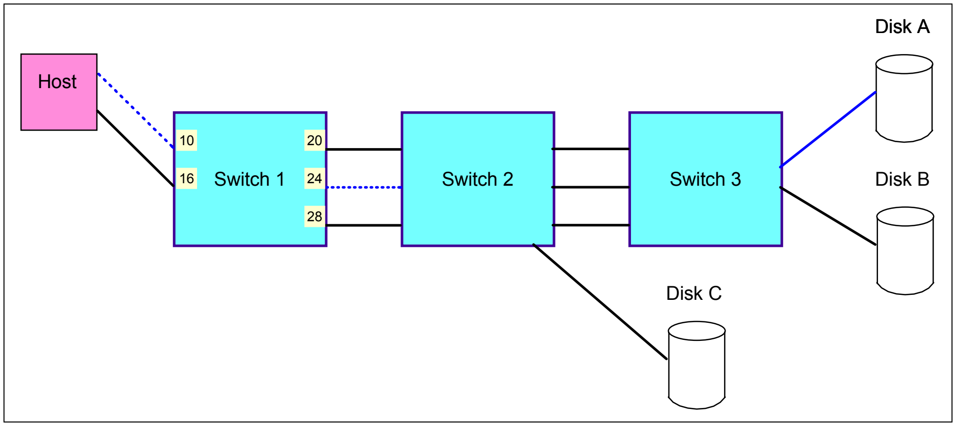

Disk A
Host
10
16
Switch 1
20
24
28
Switch 2
Switch 3
Disk B
Disk C

Figure 2-203 Preferred Path example

To configure such a route, select **Configure** → **Preferred Path...** which produces the window shown in Figure 2-204. Make sure that the **Enable Preferred Path** check box is checked, and click the **Add** button.

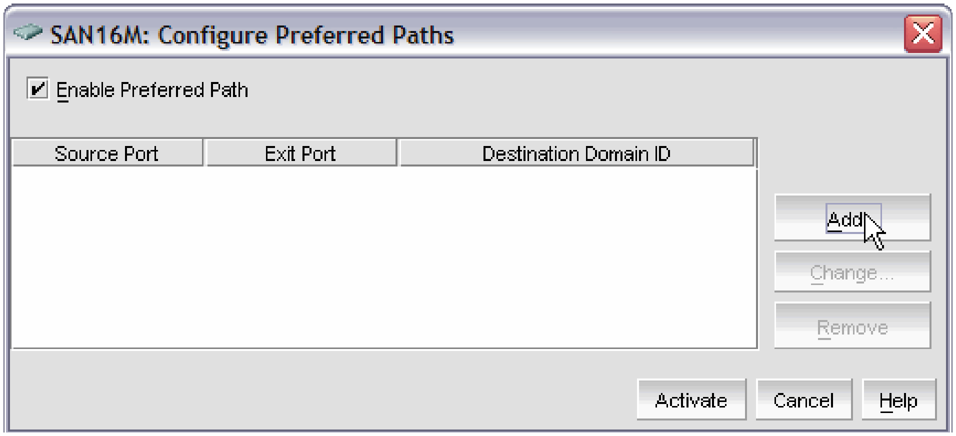
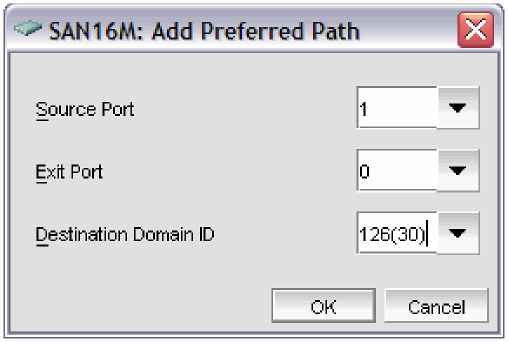

SAN16M: Configure Preferred Paths
☑ Enable Preferred Path
Source Port
Exit Port
Destination Domain ID
Add
Change...
Remove
Activate
Cancel
Help

Figure 2-204 Preferred Path dialogue box

Enter 1 for the source port, 0 for the exit port, and 126 for the destination domain ID, and click **OK** (Figure 2-205).


SAN16M: Add Preferred Path

Source Port: 1

Exit Port: 0

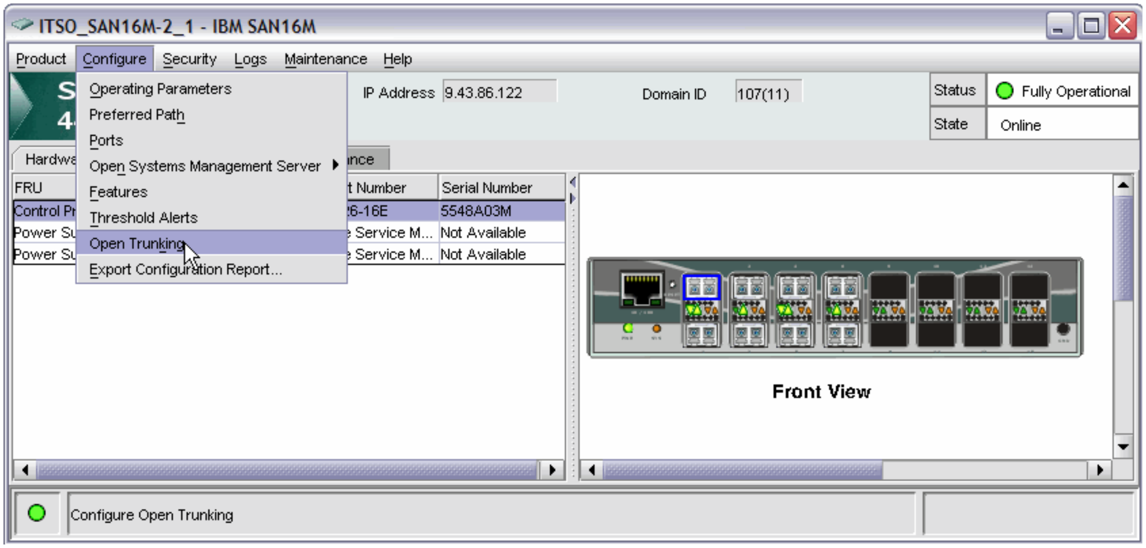
Destination Domain ID: 126(30)

Figure 2-205 Adding a preferred path

2.19.3 Open Trunking

As described in 2.3.5, “Open Trunking” on page 391, the trunking implementation on m-type switches works by load balancing ISL traffic exiting a switch. The user can enable/disable Open Trunking on the switch, and configure the settings for congestion thresholds (per port) and the low BB_Credit threshold for fine tuning purposes if required.

Launch the switch Element Manager from the EFCM client and select **Configure** → **Open Trunking...** as shown in Figure 2-206.


ITSO_SAN16M-2_1 - IBM SAN16M

IP Address: 9.43.86.122

Domain ID: 107(11)

Status: Fully Operational

State: Online

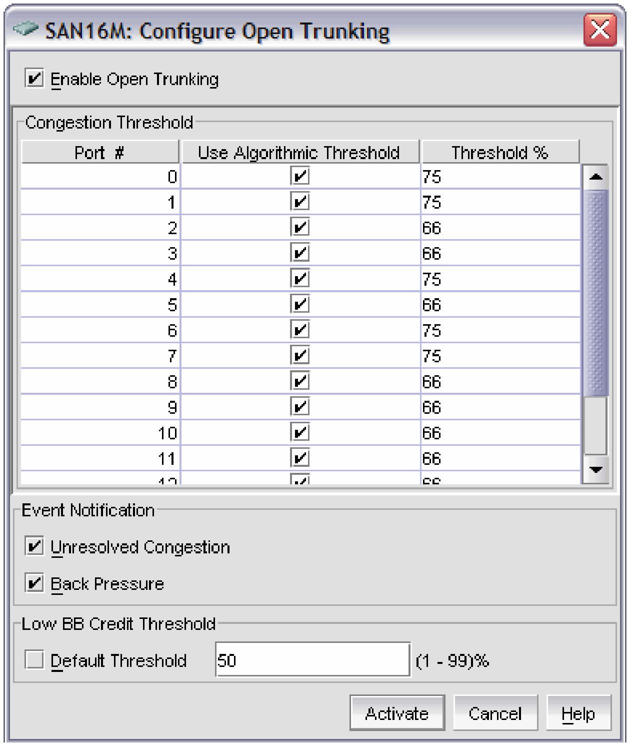
Configure Open Trunking

Product
Configure
Security
Logs
Maintenance
Help
Operating Parameters
Preferred Path
Ports
Open Systems Management Server
Features
Threshold Alerts
Open Trunking
Export Configuration Report...
Hardwa
nce
FRU
t Number
Serial Number
Control Pr
6-16E
5548A03M
Power Su
Service M...
Not Available
Power Su
Service M...
Not Available
Front View

Figure 2-206 Open Trunking

> **Attention:** This is a licensed feature, which must be installed on every switch or director that has to use it. Feature installation is covered in 2.14.12, “Feature installation and licensing” on page 458.

You open the window shown in Figure 2-207. Ensure that the **Enable Open Trunking** check box is checked to enable the feature for the switch. You might also want to enable the **Unresolved Congestion** and **Back Pressure Event Notification** features. Finally, click **Activate**.



☑ Enable Open Trunking

Congestion Threshold

Port #	Use Algorithmic Threshold	Threshold %
0	☑	75
1	☑	75
2	☑	66
3	☑	66
4	☑	75
5	☑	66
6	☑	75
7	☑	75
8	☑	66
9	☑	66
10	☑	66
11	☑	66

Event Notification

☑ Unresolved Congestion

☑ Back Pressure

Low BB Credit Threshold

☐ Default Threshold 50 (1 - 99)%

Figure 2-207 Configuring Open Trunking

Unresolved Congestion Event Notification

An unresolved congestion event occurs when the rerouting algorithm cannot find a path for rerouting data flow and relieving congestion on an ISL. The first time such an event occurs, an entry is made to the Event Log and an SNMP is generated if trap recipients are configured. Notifications are not resent while the problem persists.

Back Pressure Event Notification

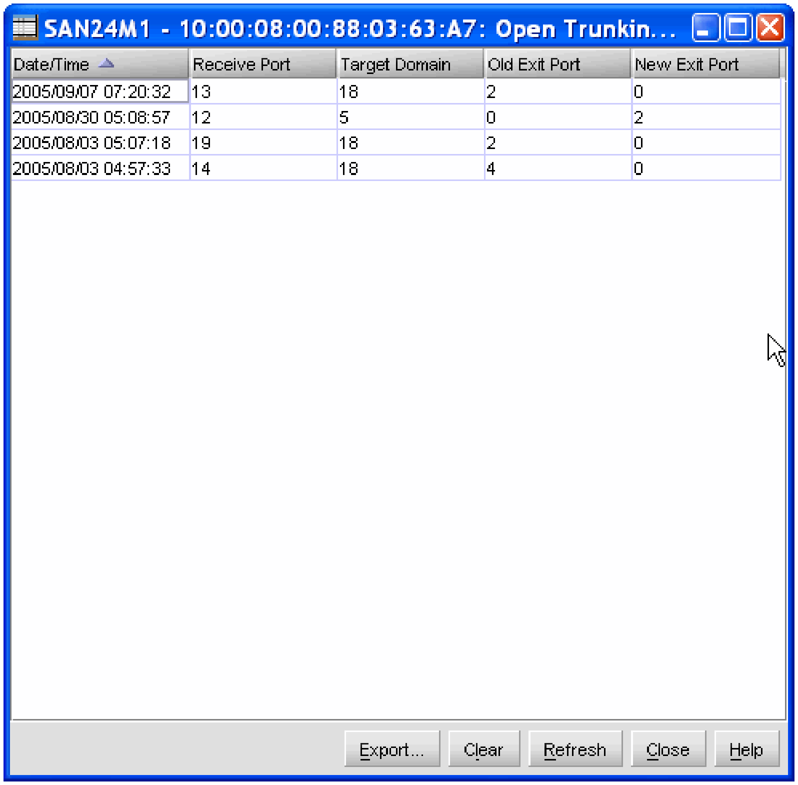
A back pressure event occurs when the percentage of time in which the ISL has no available BB_Credit exceeds the Low BB Credit threshold. A separate event also occurs when the back pressure condition ends. The first time such an event occurs, an entry is made to the Event Log and an SNMP is generated if trap recipients are configured. Notifications are not resent while the problem persists.

More detail regarding fine-tuning the other options can be found at the Web site:

`http://www.mcdata.com/knowcenter/techpubs/index.html`

Open Trunking log

The Open Trunking log is available from the EFC Element Manager and shows log flow redistribution data. From the EFC Element Manager, select the **Logs** → **Open Trunking Log...** option, and the window that opens will list data for any rerouting experienced on the director or switch, as shown in Figure 2-208.



Date/Time	Receive Port	Target Domain	Old Exit Port	New Exit Port
2005/09/07 07:20:32	13	18	2	0
2005/08/30 05:08:57	12	5	0	2
2005/08/03 05:07:18	19	18	2	0
2005/08/03 04:57:33	14	18	4	0

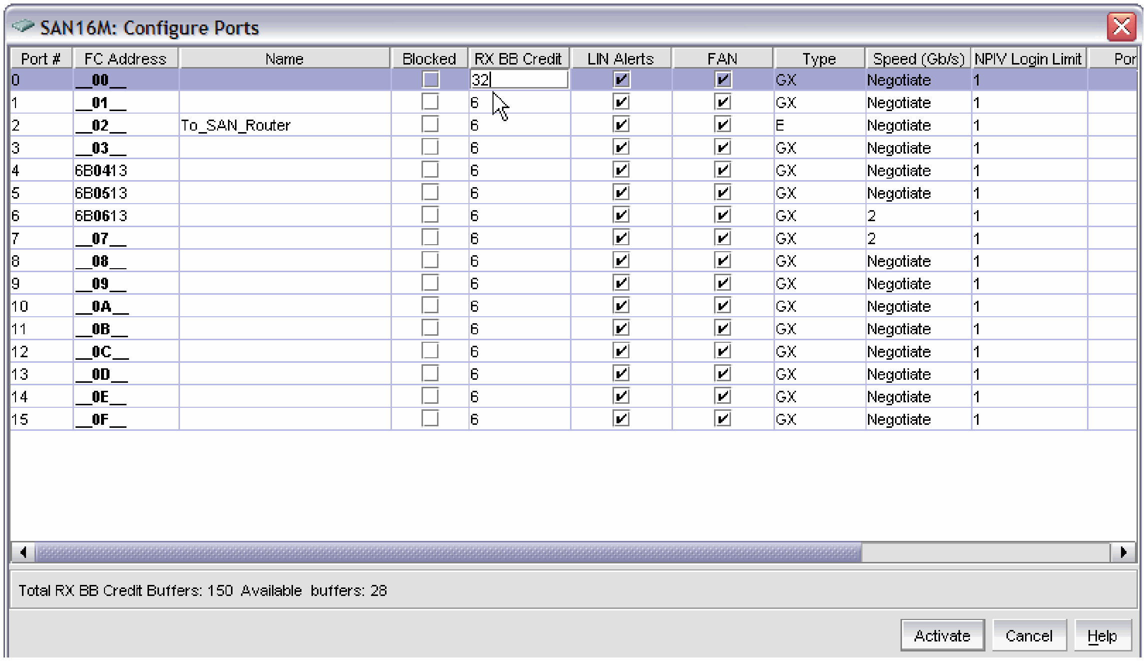
Figure 2-208 Open Trunking log

2.19.4 Long distance

Shortwave optics support distances of a couple of hundred metres (depending on link speed), while standard longwave optics enable distances up to 10 kilometres. With extended longwave optics, this can be stretched to 20 or 35 kilometres. Using optical repeaters can extend this further, but for true long distance, a separate routing device such as the IBM TotalStorage SAN04M-R is required.

The important thing to remember with increased distances is that the number of buffer-to-buffer credits has to increase to accommodate the increased link transmission times. As a rough guide, for a 2 Gbps link, one BB_Credit is required per kilometre.

To adjust the number of BB_Credits for a given port, select **Configure → Ports...** and over-type the number in the RX BB Credit column, as shown in Figure 2-209. The number of unallocated buffers is displayed at the bottom of the window.



Port #	FC Address	Name	Blocked	RX BB Credit	LIN Alerts	FAN	Type	Speed (Gb/s)	NPIV Login Limit	Por
0	__00__		☐	32	☑	☑	GX	Negotiate	1	
1	__01__		☐	6	☑	☑	GX	Negotiate	1	
2	__02__	To_SAN_Router	☐	6	☑	☑	E	Negotiate	1	
3	__03__		☐	6	☑	☑	GX	Negotiate	1	
4	6B0413		☐	6	☑	☑	GX	Negotiate	1	
5	6B0513		☐	6	☑	☑	GX	Negotiate	1	
6	6B0613		☐	6	☑	☑	GX	2	1	
7	__07__		☐	6	☑	☑	GX	2	1	
8	__08__		☐	6	☑	☑	GX	Negotiate	1	
9	__09__		☐	6	☑	☑	GX	Negotiate	1	
10	__0A__		☐	6	☑	☑	GX	Negotiate	1	
11	__0B__		☐	6	☑	☑	GX	Negotiate	1	
12	__0C__		☐	6	☑	☑	GX	Negotiate	1	
13	__0D__		☐	6	☑	☑	GX	Negotiate	1	
14	__0E__		☐	6	☑	☑	GX	Negotiate	1	
15	__0F__		☐	6	☑	☑	GX	Negotiate	1	

Total RX BB Credit Buffers: 150 Available buffers: 28

Figure 2-209 Adjusting port BB_Credits

It is important to remember with long distance ISLs that the performance of the fabric can be affected when fabric configuration events occur. This can be avoided by the use of a router which enables the two ends of the link to be operated as separate fabrics, and only defined traffic routed between them.

2.19.5 Merging

Several criteria must match for two fabrics to successfully merge, including these:

- The R_A_TOV and E_D_TOV values must match.
- The interop modes must match.
- If the Insistent domain setting is used, there must be no domain ID conflicts.
- The active zone sets must be compatible, as they will be merged.

If any of these criteria are not met, the ISLs joining the two fabrics will segment, and no traffic will flow other than management traffic.

Zones are compatible if:

- Active zones have unique names
- Active zones have identical names and have the same zone members

2.19.6 Routing and iFCP

Routing, either over FC-FC or iFCP, can only be achieved via a separate SAN router such as the IBM TotalStorage SAN16M-R or SAN04M-R multiprotocol SAN routers, which are described in *SAN Multiprotocol Routing: An Introduction and Implementation*, SG24-73211.

2.20 iSCSI

iSCSI is supported through the use of the IBM TotalStorage SAN16M-R or SAN04M-R multiprotocol SAN routers, which are described in *SAN Multiprotocol Routing: An Introduction and Implementation*, SG24-73211.

2.21 FICON

FICON is a protocol used by IBM zSeries processors and is the follow-on to ESCON®. It exploits the same physical SAN infrastructure as FCP, and can share the same switches and directors — this is known as inter-mix. While no special configuration of switch ports is required to support FICON, a storage or host N_Port can only operate in FCP or FICON mode.

zSeries hosts do not use the SAN name service to discover the nodes they are authorized to, but instead use a processor configuration file to define their connectivity. As such, it is only necessary to place all FICON ports in a single zone to isolate them from FCP traffic.

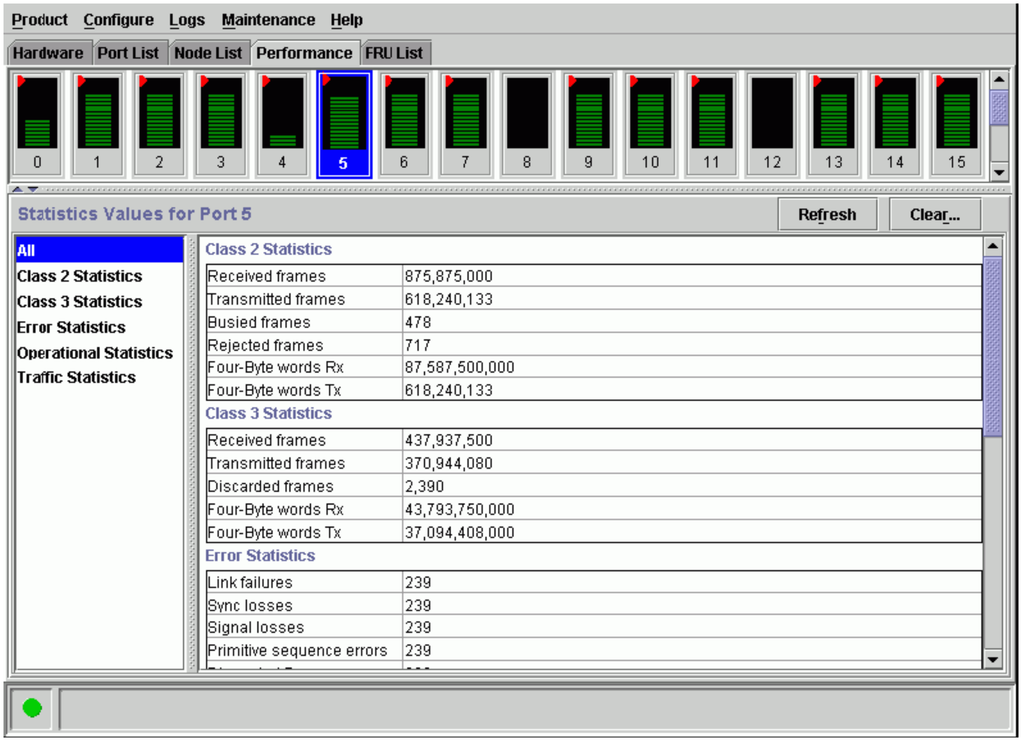
Tip: Installation of the FICON Management Server (CUP) feature is not required to support FICON traffic. It is only required for in-band management from zSeries hosts.

2.22 Performance monitoring

In the topics that follow, we introduce performance monitoring.

2.22.1 Real-time

Real-time performance monitoring of switch ports is provided as standard via the Element Manager *Performance* tab. This allows for a group of ports to be monitored in the form of small bar charts, and in addition, detailed statistics to be displayed for one of the ports at a time. An example of monitoring port 5 is shown in Figure 2-210.


Product
Configure
Logs
Maintenance
Help
Hardware
Port List
Node List
Performance
FRU List
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Statistics Values for Port 5
Refresh
Clear...
All
Class 2 Statistics
Class 3 Statistics
Error Statistics
Operational Statistics
Traffic Statistics

Class 2 Statistics

Received frames	875,875,000
Transmitted frames	618,240,133
Busied frames	478
Rejected frames	717
Four-Byte words Rx	87,587,500,000
Four-Byte words Tx	618,240,133

Class 3 Statistics

Received frames	437,937,500
Transmitted frames	370,944,080
Discarded frames	2,390
Four-Byte words Rx	43,793,750,000
Four-Byte words Tx	37,094,408,000

Error Statistics

Link failures	239
Sync losses	239
Signal losses	239
Primitive sequence errors	239

Figure 2-210 Real-time port performance monitoring

2.22.2 Historic

In addition, if you have the Performance Monitoring feature licensed on your EFCM server, the server can be configured to record performance data for the switches and directors it manages. To enable recording, select **Monitor** → **Performance** → **Setup** as shown in Figure 2-211.

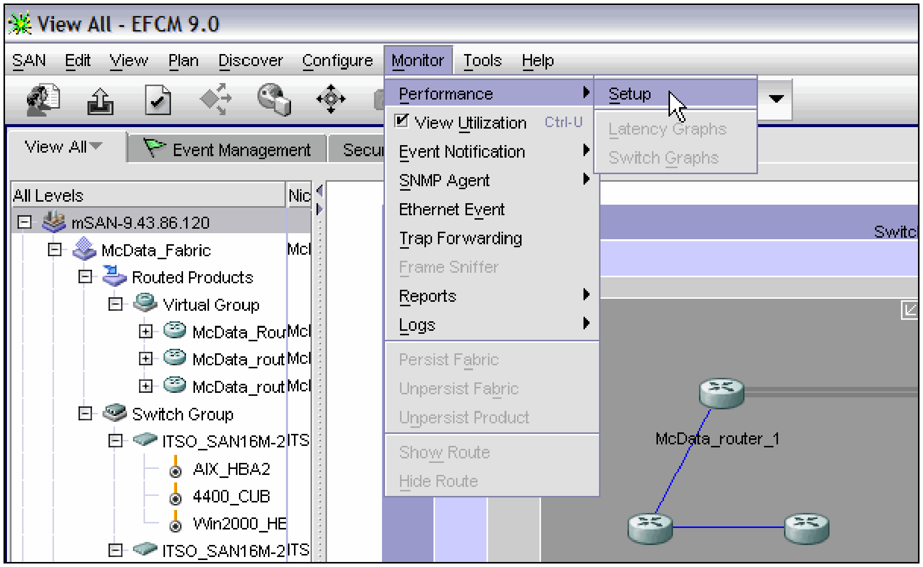
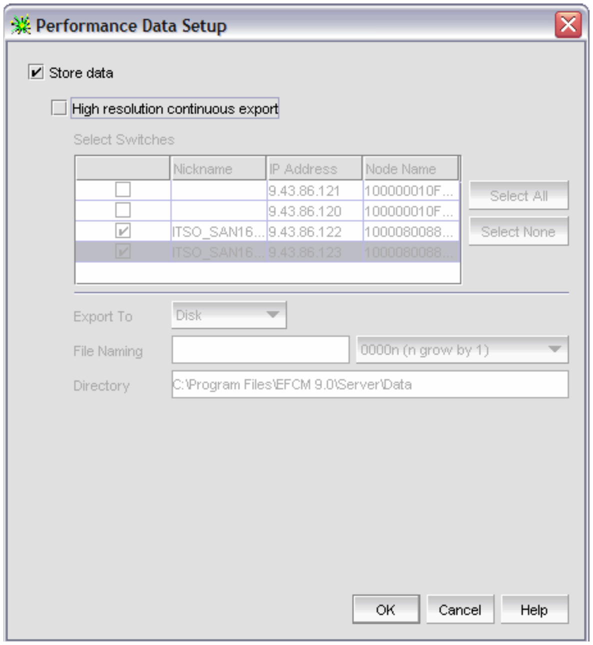

View All - EFCM 9.0
SAN
Edit
View
Plan
Discover
Configure
Monitor
Tools
Help
Performance
View Utilization Ctrl-U
Event Notification
SNMP Agent
Ethernet Event
Trap Forwarding
Frame Sniffer
Reports
Logs
Persist Fabric
Unpersist Fabric
Unpersist Product
Show Route
Hide Route
Setup
Latency Graphs
Switch Graphs
View All
Event Management
All Levels
mSAN-9.43.86.120
McData_Fabric
Routed Products
Virtual Group
McData_Rou
McData_rout
McData_rout
Switch Group
ITSO_SAN16M-2
AIX_HBA2
4400_CUB
Win2000_HE
ITSO_SAN16M-2
McData_router_1

Figure 2-211 Enabling switch performance recording

Now ensure that the **Store Data** check box is checked, as shown in Figure 2-212.


Performance Data Setup
Select Switches
Select All
Select None
OK
Cancel
Help

☑ Store data

☐ High resolution continuous export

	Nickname	IP Address	Node Name
☐		9.43.86.121	100000010F...
☐		9.43.86.120	100000010F...
☑	ITSO_SAN16...	9.43.86.122	1000080088...
☑	ITSO_SAN16...	9.43.86.123	1000080088...

Export To: Disk

File Naming: 0000n (n grow by 1)

Directory: C:\Program Files\EFCM 9.0\Server\Data

Figure 2-212 Performance Data Setup

To generate a report, select **Monitor** → **Reports** → **Generate Reports**, check the **Performance Data** check box and click **OK**, as shown in Figure 2-213.

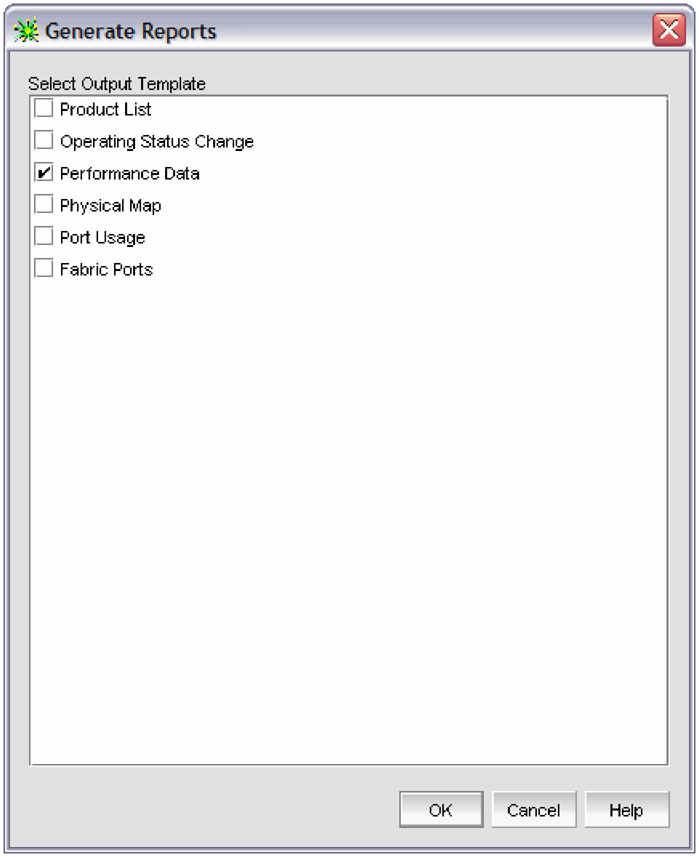
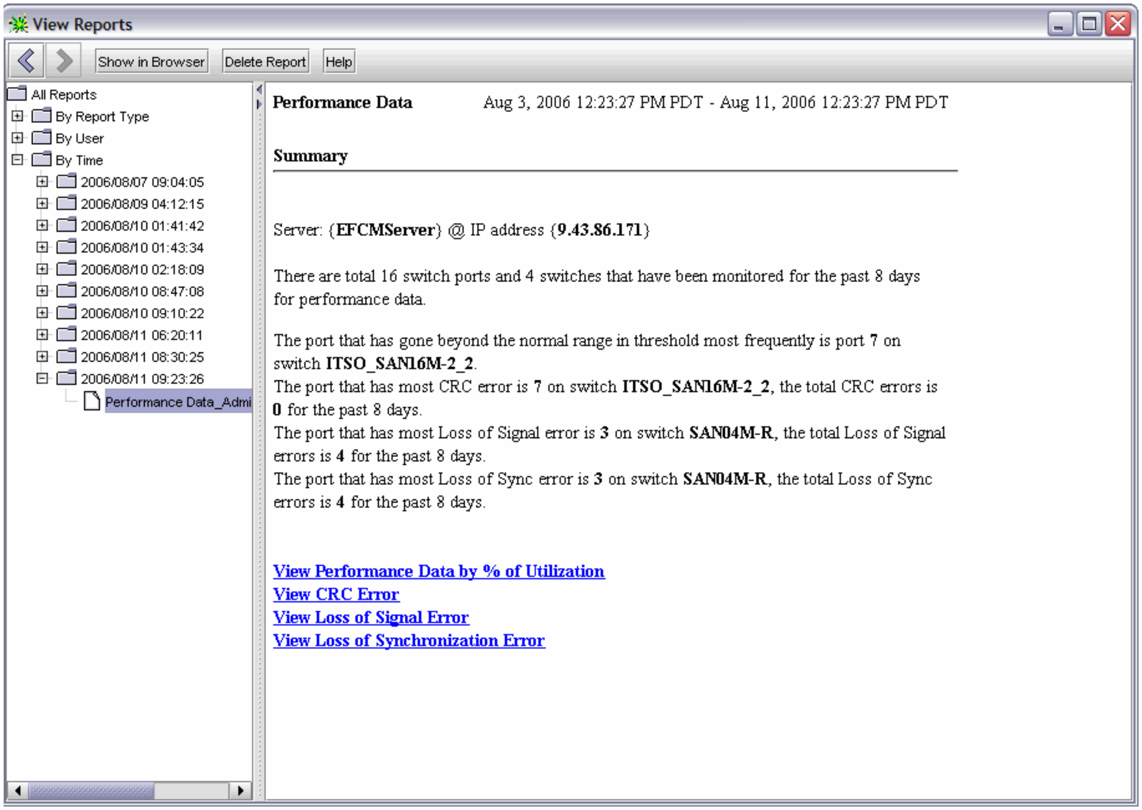

Generate Reports
Select Output Template
☐ Product List
☐ Operating Status Change
☑ Performance Data
☐ Physical Map
☐ Port Usage
☐ Fabric Ports
OK
Cancel
Help

Figure 2-213 Selecting performance report

The *Reports* window shown in Figure 2-214 opens automatically. You can then look into more detail of this report by selecting the underlined highlighted links on this page.


View Reports
Show in Browser
Delete Report
Help
All Reports
By Report Type
By User
By Time
2006/08/07 09:04:05
2006/08/09 04:12:15
2006/08/10 01:41:42
2006/08/10 01:43:34
2006/08/10 02:18:09
2006/08/10 08:47:08
2006/08/10 09:10:22
2006/08/11 06:20:11
2006/08/11 08:30:25
2006/08/11 09:23:26
Performance Data_Admi

Performance Data Aug 3, 2006 12:23:27 PM PDT - Aug 11, 2006 12:23:27 PM PDT

Summary

Server: {**EFCMServer**} @ IP address {**9.43.86.171**}

There are total 16 switch ports and 4 switches that have been monitored for the past 8 days for performance data.

The port that has gone beyond the normal range in threshold most frequently is port **7** on switch **ITSO_SAN16M-2_2**.
The port that has most CRC error is **7** on switch **ITSO_SAN16M-2_2**, the total CRC errors is **0** for the past 8 days.
The port that has most Loss of Signal error is **3** on switch **SAN04M-R**, the total Loss of Signal errors is **4** for the past 8 days.
The port that has most Loss of Sync error is **3** on switch **SAN04M-R**, the total Loss of Sync errors is **4** for the past 8 days.

View Performance Data by % of Utilization
View CRC Error
View Loss of Signal Error
View Loss of Synchronization Error

Figure 2-214 Performance report window

2.22.3 Performance graph

The Performance Monitoring feature also provides the facility to display graphs of port activity over various time intervals.

This is done by right-clicking a switch icon and selecting **Performance Graphs** from the pop-up menu, as shown in Figure 2-215.

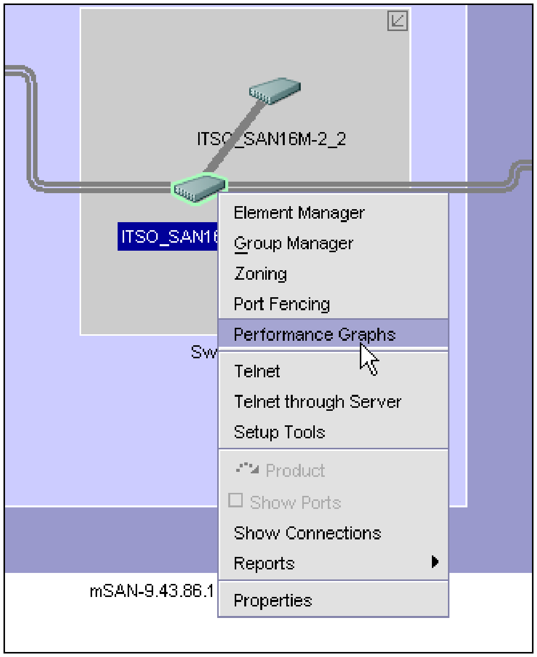
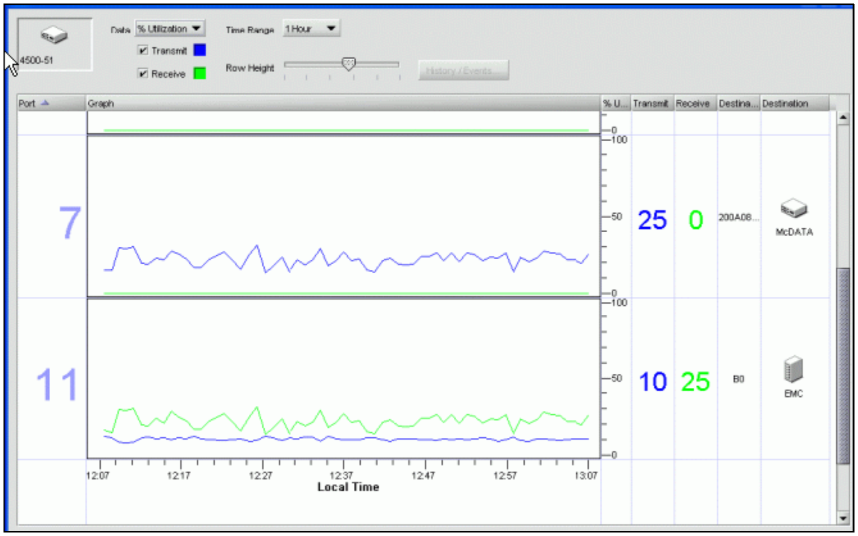

ITSO_SAN16M-2_2
ITSO_SAN16
Sw
mSAN-9.43.86.1
Element Manager
Group Manager
Zoning
Port Fencing
Performance Graphs
Telnet
Telnet through Server
Setup Tools
Product
☐ Show Ports
Show Connections
Reports
Properties

Figure 2-215 Selecting Performance Graphs

The example in Figure 2-216 shows the transmit and receive utilization for two ports during one hour.


4500-51

Data: % Utilization

☑ Transmit 🟦

☑ Receive 🟩

Time Range: 1 Hour

Port	% U...	Transmit	Receive	Destina...	Destination
7		25	0	200A08...	McDATA
11		10	25	B0	EMC

Row Height
History / Events...
Graph
0
100
50
0
100
50
0
12:07
12:17
12:27
12:37
12:47
12:57
13:07
Local Time

Figure 2-216 Switch performance graph

More detail on this feature can be found in the *McDATA EFC Manager Performance User Manual*, 620-000165.

2.23 Basic troubleshooting

In the sections that follow, we show some of the ways in which you can troubleshoot the SAN.

There are a few basic questions used in troubleshooting SAN problems.

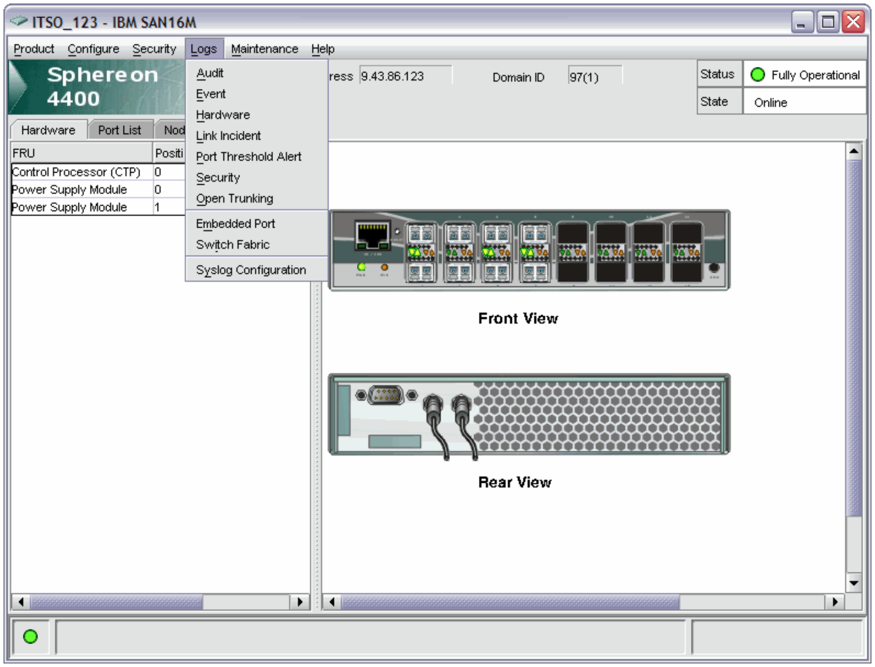
- Is the problem effecting only one host?
- Is the problem effecting only one storage device?
- Is the problem only on one SAN switch?
- Can the SAN be managed? Are all devices seen on EFCM?
- Has there been any change at all on the SAN?
- Is the problem visible, such as an error indicator, or an error shown on EFCM?

By answering these questions, we can narrow our search for the cause of the problem and concentrate on fixing the problem.

2.23.1 Logs

Usually the first step in SAN problem determination is to check for any alerts. If alerts are detected, the alert details should be checked. After this, the appropriate logs should be examined. Some logs are part of the EFCM application, and each director or switch also has its own logs viewable via the Element Manager.

The logs can be accessed from the Element Manager by selecting **Logs** from the menu as shown in Figure 2-217.


ITSO_123 - IBM SAN16M
Product
Configure
Security
Logs
Maintenance
Help
Sphereon 4400
Audit
Event
Hardware
Link Incident
Port Threshold Alert
Security
Open Trunking
Embedded Port
Switch Fabric
Syslog Configuration
Hardware
Port List
Nod
Front View
Rear View

ress 9.43.86.123

Domain ID 97(1)

Status: Fully Operational

State: Online

FRU	Positi
Control Processor (CTP)	0
Power Supply Module	0
Power Supply Module	1

Figure 2-217 Log selection from Element Manager

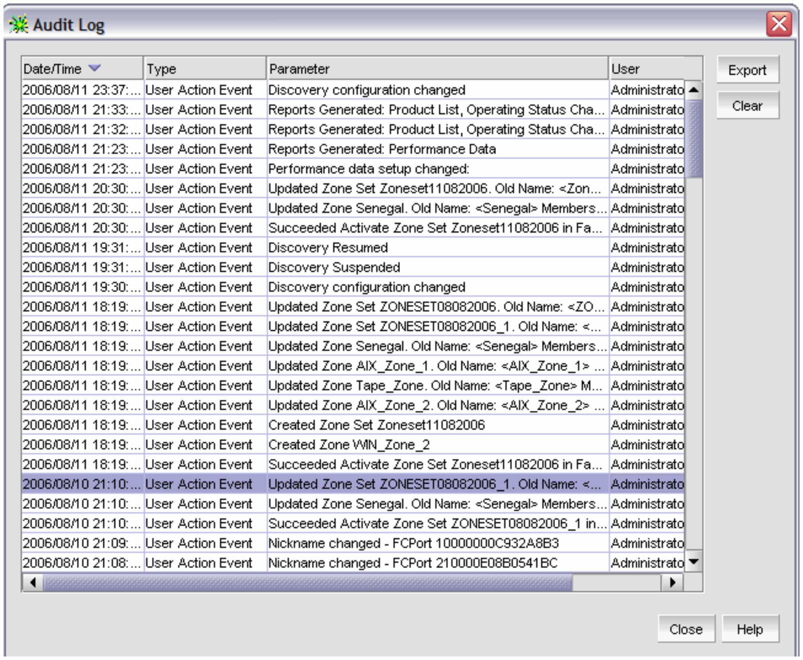
EFCM logs

The EFCM has several logs, which we describe in the following sections.

- Audit
- Event
- Fabric
- Group
- Product status
- Security
- Session

Audit log

This log displays a history of user actions performed through the application (except login/logout). These logs can be useful to determine if there was a change in the fabric, as shown in Figure 2-218. This log shows any changes and which user performed each change.



Date/Time	Type	Parameter	User
2006/08/11 23:37:...	User Action Event	Discovery configuration changed	Administrato
2006/08/11 21:33:...	User Action Event	Reports Generated: Product List, Operating Status Cha...	Administrato
2006/08/11 21:32:...	User Action Event	Reports Generated: Product List, Operating Status Cha...	Administrato
2006/08/11 21:23:...	User Action Event	Reports Generated: Performance Data	Administrato
2006/08/11 21:23:...	User Action Event	Performance data setup changed:	Administrato
2006/08/11 20:30:...	User Action Event	Updated Zone Set Zoneset11082006. Old Name: <Zon...	Administrato
2006/08/11 20:30:...	User Action Event	Updated Zone Senegal. Old Name: <Senegal> Members...	Administrato
2006/08/11 20:30:...	User Action Event	Succeeded Activate Zone Set Zoneset11082006 in Fa...	Administrato
2006/08/11 19:31:...	User Action Event	Discovery Resumed	Administrato
2006/08/11 19:31:...	User Action Event	Discovery Suspended	Administrato
2006/08/11 19:30:...	User Action Event	Discovery configuration changed	Administrato
2006/08/11 18:19:...	User Action Event	Updated Zone Set ZONESET08082006. Old Name: <ZO...	Administrato
2006/08/11 18:19:...	User Action Event	Updated Zone Set ZONESET08082006_1. Old Name: <...	Administrato
2006/08/11 18:19:...	User Action Event	Updated Zone Senegal. Old Name: <Senegal> Members...	Administrato
2006/08/11 18:19:...	User Action Event	Updated Zone AIX_Zone_1. Old Name: <AIX_Zone_1> ...	Administrato
2006/08/11 18:19:...	User Action Event	Updated Zone Tape_Zone. Old Name: <Tape_Zone> M...	Administrato
2006/08/11 18:19:...	User Action Event	Updated Zone AIX_Zone_2. Old Name: <AIX_Zone_2> ...	Administrato
2006/08/11 18:19:...	User Action Event	Created Zone Set Zoneset11082006	Administrato
2006/08/11 18:19:...	User Action Event	Created Zone WIN_Zone_2	Administrato
2006/08/11 18:19:...	User Action Event	Succeeded Activate Zone Set Zoneset11082006 in Fa...	Administrato
2006/08/10 21:10:...	User Action Event	Updated Zone Set ZONESET08082006_1. Old Name: <...	Administrato
2006/08/10 21:10:...	User Action Event	Updated Zone Senegal. Old Name: <Senegal> Members...	Administrato
2006/08/10 21:10:...	User Action Event	Succeeded Activate Zone Set ZONESET08082006_1 in...	Administrato
2006/08/10 21:09:...	User Action Event	Nickname changed - FCPort 10000000C932A8B3	Administrato
2006/08/10 21:08:...	User Action Event	Nickname changed - FCPort 210000E08B0541BC	Administrato

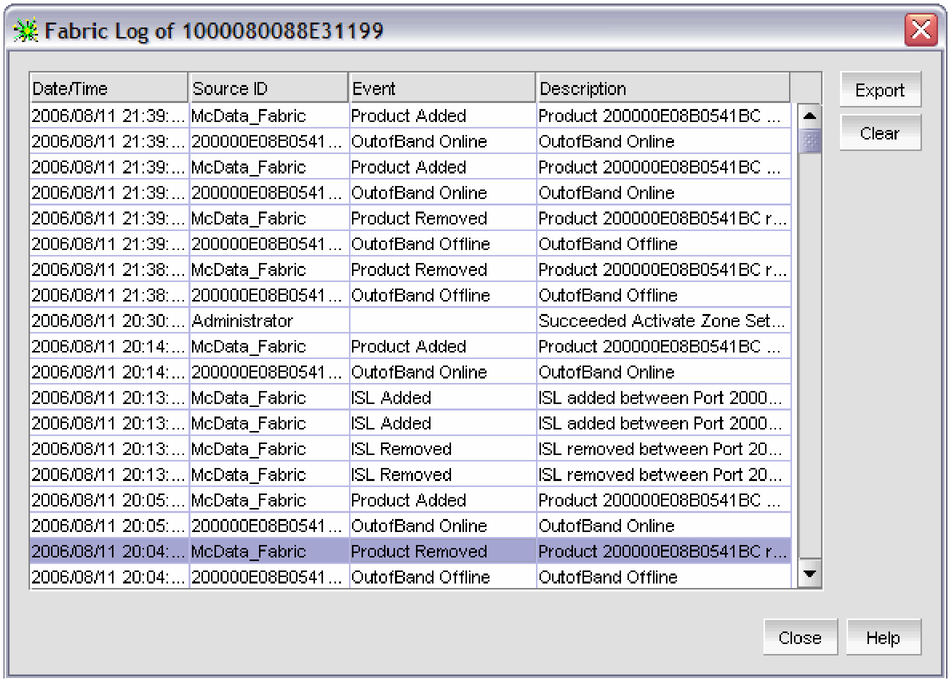
Figure 2-218 Audit log

Event log

This log displays errors related to SNMP traps and Client-Server communications.

Fabric log

This log displays events that have occurred for a selected fabric. To display the log, you must have persisted the fabric through the Persist Fabric dialog box. You must also select the persisted fabric from the Physical Map before selecting Fabric Log from the menu. This is a useful log because it shows any change to the fabric, as shown in Figure 2-219.



Date/Time	Source ID	Event	Description
2006/08/11 21:39:...	McData_Fabric	Product Added	Product 200000E08B0541BC ...
2006/08/11 21:39:...	200000E08B0541 ...	OutofBand Online	OutofBand Online
2006/08/11 21:39:...	McData_Fabric	Product Added	Product 200000E08B0541BC ...
2006/08/11 21:39:...	200000E08B0541 ...	OutofBand Online	OutofBand Online
2006/08/11 21:39:...	McData_Fabric	Product Removed	Product 200000E08B0541BC r...
2006/08/11 21:39:...	200000E08B0541 ...	OutofBand Offline	OutofBand Offline
2006/08/11 21:38:...	McData_Fabric	Product Removed	Product 200000E08B0541BC r...
2006/08/11 21:38:...	200000E08B0541 ...	OutofBand Offline	OutofBand Offline
2006/08/11 20:30:...	Administrator		Succeeded Activate Zone Set...
2006/08/11 20:14:...	McData_Fabric	Product Added	Product 200000E08B0541BC ...
2006/08/11 20:14:...	200000E08B0541 ...	OutofBand Online	OutofBand Online
2006/08/11 20:13:...	McData_Fabric	ISL Added	ISL added between Port 2000...
2006/08/11 20:13:...	McData_Fabric	ISL Added	ISL added between Port 2000...
2006/08/11 20:13:...	McData_Fabric	ISL Removed	ISL removed between Port 20...
2006/08/11 20:13:...	McData_Fabric	ISL Removed	ISL removed between Port 20...
2006/08/11 20:05:...	McData_Fabric	Product Added	Product 200000E08B0541BC ...
2006/08/11 20:05:...	200000E08B0541 ...	OutofBand Online	OutofBand Online
2006/08/11 20:04:...	McData_Fabric	Product Removed	Product 200000E08B0541BC r...
2006/08/11 20:04:...	200000E08B0541 ...	OutofBand Offline	OutofBand Offline

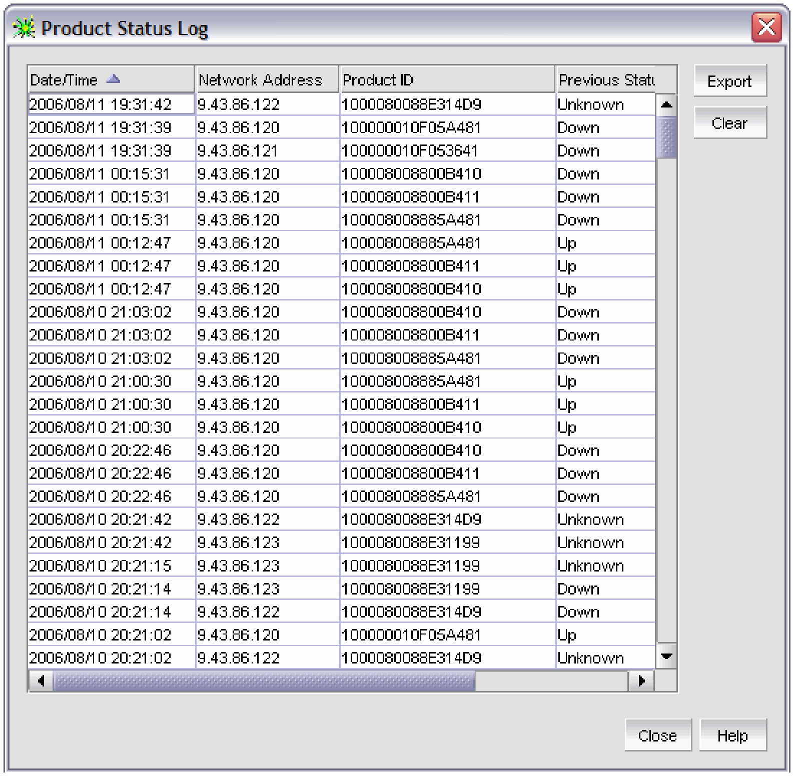
Figure 2-219 Fabric Log

Group log

This log displays the event logs defined on the Group Management window.

Product status log

This log displays operational status changes of managed products as shown in Figure 2-220.



Date/Time	Network Address	Product ID	Previous Statu
2006/08/11 19:31:42	9.43.86.122	1000080088E314D9	Unknown
2006/08/11 19:31:39	9.43.86.120	100000010F05A481	Down
2006/08/11 19:31:39	9.43.86.121	100000010F053641	Down
2006/08/11 00:15:31	9.43.86.120	100008008800B410	Down
2006/08/11 00:15:31	9.43.86.120	100008008800B411	Down
2006/08/11 00:15:31	9.43.86.120	100008008885A481	Down
2006/08/11 00:12:47	9.43.86.120	100008008885A481	Up
2006/08/11 00:12:47	9.43.86.120	100008008800B411	Up
2006/08/11 00:12:47	9.43.86.120	100008008800B410	Up
2006/08/10 21:03:02	9.43.86.120	100008008800B410	Down
2006/08/10 21:03:02	9.43.86.120	100008008800B411	Down
2006/08/10 21:03:02	9.43.86.120	100008008885A481	Down
2006/08/10 21:00:30	9.43.86.120	100008008885A481	Up
2006/08/10 21:00:30	9.43.86.120	100008008800B411	Up
2006/08/10 21:00:30	9.43.86.120	100008008800B410	Up
2006/08/10 20:22:46	9.43.86.120	100008008800B410	Down
2006/08/10 20:22:46	9.43.86.120	100008008800B411	Down
2006/08/10 20:22:46	9.43.86.120	100008008885A481	Down
2006/08/10 20:21:42	9.43.86.122	1000080088E314D9	Unknown
2006/08/10 20:21:42	9.43.86.123	1000080088E31199	Unknown
2006/08/10 20:21:15	9.43.86.123	1000080088E31199	Unknown
2006/08/10 20:21:14	9.43.86.123	1000080088E31199	Down
2006/08/10 20:21:14	9.43.86.122	1000080088E314D9	Down
2006/08/10 20:21:02	9.43.86.120	100000010F05A481	Up
2006/08/10 20:21:02	9.43.86.122	1000080088E314D9	Unknown

Figure 2-220 Product status log

Security log

This log displays security related events that have occurred.

Session log

This log displays the users who have logged in and out of the server.

Master log

The Master Log, which displays in the lower left area of the main window, lists all events from the Element Manager and EFCM logs that occurred throughout the SAN. These include user actions, client/server communications, SNMP trap errors, product hardware errors, product link incident and threshold errors, and Ethernet events. This log combines entries from all other EFC Manager and Element Manager logs. Pressing the PF5 key also opens the Master Log into the main window.

Element Manager logs

EFCM has several logs, which we describe in the following sections. You select these by selecting **Monitor** → **Logs** as shown in Figure 2-221.

- Audit
- Event
- Hardware
- Link incident
- Threshold alert
- Security
- Open Trunking
- Advanced
  - Embedded port
  - Switch fabric

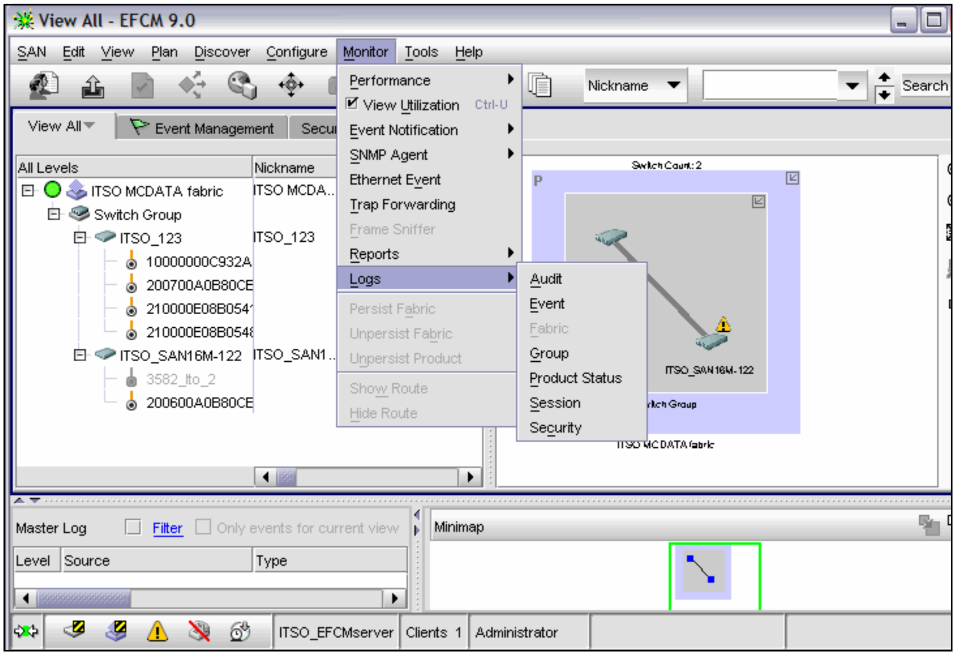

View All - EFCM 9.0
SAN
Edit
View
Plan
Discover
Configure
Monitor
Tools
Help
Performance
View Utilization Ctrl-U
Event Notification
SNMP Agent
Ethernet Event
Trap Forwarding
Frame Sniffer
Reports
Logs
Persist Fabric
Unpersist Fabric
Unpersist Product
Show Route
Hide Route
Audit
Event
Fabric
Group
Product Status
Session
Security
Nickname
Search
View All
Event Management
All Levels
ITSO MCDATA fabric
Switch Group
ITSO_123
10000000C932A
200700A0B80CE
210000E08B054
210000E08B054
ITSO_SAN16M-122
3582_lto_2
200600A0B80CE
Switch Count: 2
ITSO_SAN16M-122
Switch Group
ITSO MCDATA fabric
Master Log
Filter
Only events for current view
Level
Source
Type
Minimap
ITSO_EFCMserver
Clients 1
Administrator

Figure 2-221 Log selection from EFCM

Audit log

This log displays a history of all configuration changes applied from any source.

Event log

This log provides a record of significant events that have occurred on the switch, such as hardware failures, degraded operation, port problems, FRU failures, FRU removals and replacements, Fibre Channel link incidents, and communication problems between the switch and the server platform. The information is useful to maintenance personnel for fault isolation and repair verification.

Hardware log

This log displays information on FRUs inserted and removed from the switch.

Link incident log

This log displays a thousand of the most recent link incidents. The information is useful to maintenance personnel for isolating port problems (particularly expansion port (E_Port) segmentation problems) and repair verification.

Threshold alert

This log provides details of threshold alert notifications. Besides the date and time that the alert occurred, the log also displays details about the alert as configured through the **Threshold Alerts...** option on the **Configure** menu.

Security log

This log displays security information.

Open Trunking log

This log provides details on flow rerouting that is occurring through switch ports.

Embedded port log

This log provides a detailed history log of all traffic passing through the embedded port. The Embedded Port (EP) of the switch is an internal FC port within the hardware architecture that is used to communicate FC frames between devices attached to the external ports and the embedded firmware’s FC services software, based on the use of well-known Fibre Channel addresses. The Embedded Port Log will log all FC frame traffic directed to the switch (EP), including discards, frames not routed, and traffic designated for the EP (in-band traffic).

Switch fabric log

This log displays information about switches in a fabric.

2.23.2 Identifying and resolving hardware symptoms

In this section, we identify products that have their attention indicator on (indicating a problem) and then show the steps taken to identify and resolve the cause.

In Figure 2-222 we can see from the EFCM that an ED-6064 director and an ES-3016 require attention in this environment.

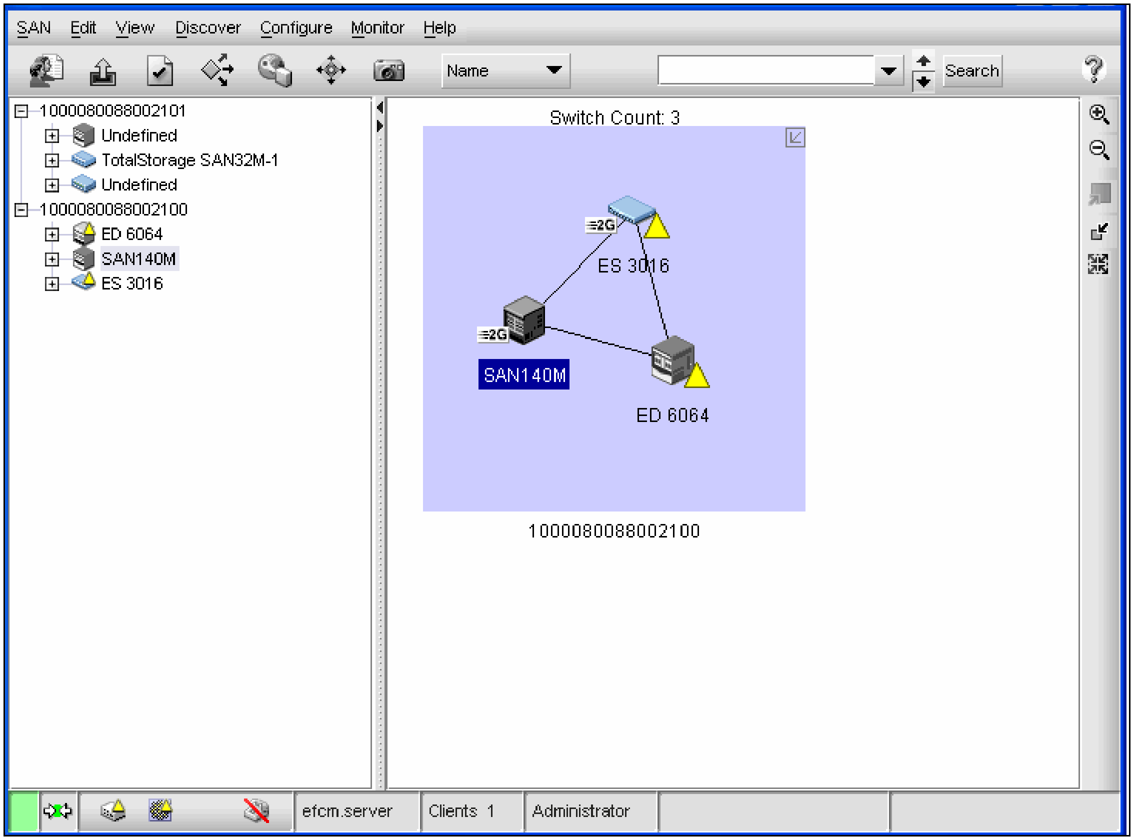
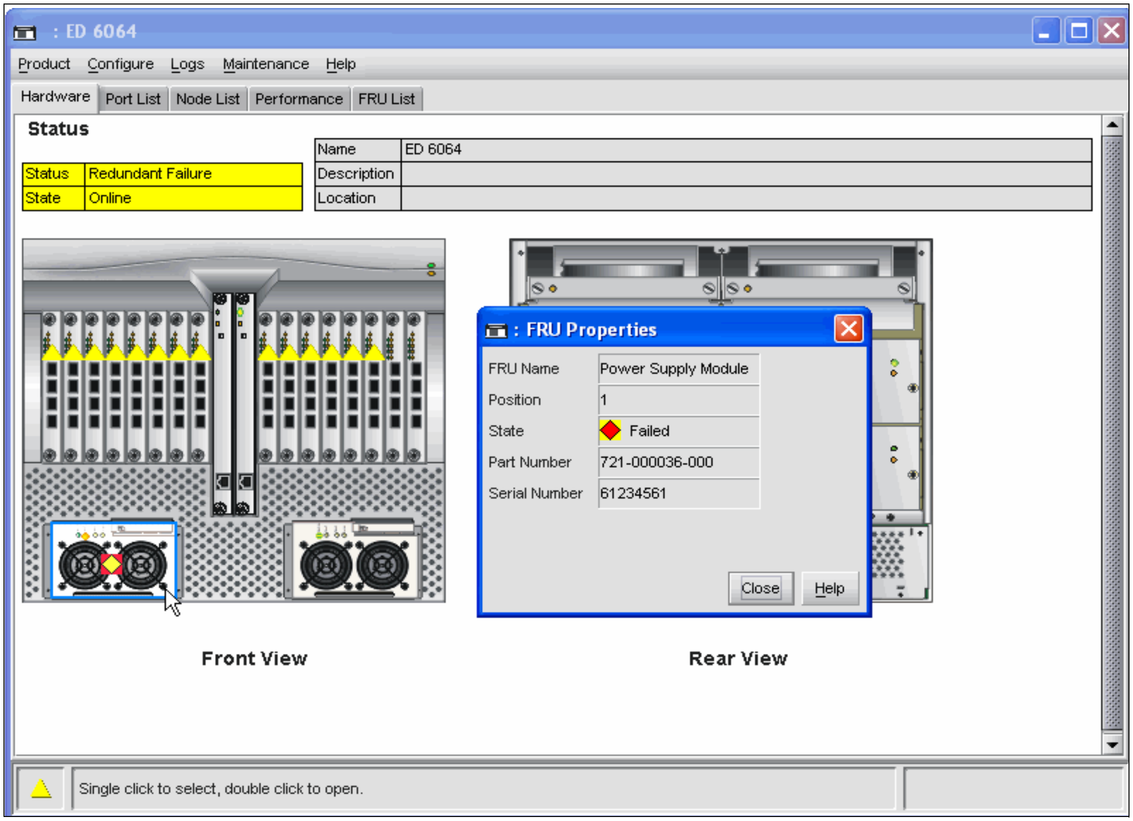

SAN
Edit
View
Discover
Configure
Monitor
Help
Name
Search
1000080088002101
Undefined
TotalStorage SAN32M-1
Undefined
1000080088002100
ED 6064
SAN140M
ES 3016
Switch Count: 3
2G
ES 3016
2G
SAN140M
ED 6064
1000080088002100
efcm.server
Clients 1
Administrator

Figure 2-222 EFCM indicating attention required


: ED 6064
Product
Configure
Logs
Maintenance
Help
Hardware
Port List
Node List
Performance
FRU List
Front View
Rear View
: FRU Properties
Close
Help

Status

Status	Redundant Failure
State	Online

Name	ED 6064
Description	
Location	

FRU Name	Power Supply Module
Position	1
State	Failed
Part Number	721-000036-000
Serial Number	61234561

Single click to select, double click to open.

Figure 2-223 Attention indicators show a failed power supply module

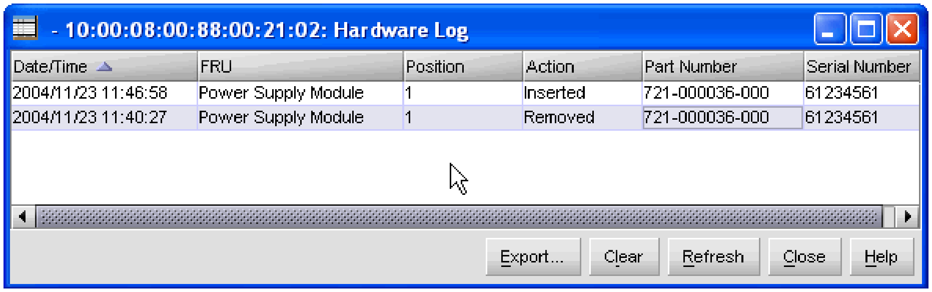
By double-clicking the ED-6064 icon, the product menu window is opened as shown in Figure 2-223.

We notice that the attention indicator is blinking on the ED-6064 power supply # 1, and by double-clicking the blinking icon, the new pop-up window lists the details of the FRU and its state. We can see that the power supply module is in a failed state and is the cause of the attention indicator.

To fix the problem and clear the attention indicator, a service call has to be placed. To open a defect call, you have to gather the device type and serial number of the ED-6064 and then initiate a call to replace the failed power supply.

The part number and serial number are shown in the FRU properties box initiated when we double-clicked the failed power supply in Figure 2-223.

You can also view the ED-6064 event log to retrieve this information as well as problem description, time of activity, and FRU-position, as shown in Figure 2-224.


- 10:00:08:00:88:00:21:02: Hardware Log
Export...
Clear
Refresh
Close
Help

Date/Time	FRU	Position	Action	Part Number	Serial Number
2004/11/23 11:46:58	Power Supply Module	1	Inserted	721-000036-000	61234561
2004/11/23 11:40:27	Power Supply Module	1	Removed	721-000036-000	61234561

Figure 2-224 Maintenance log indicates problem

After installing the new power supply, the attention indicator disappears and the power redundancy in the ED-6064 is restored as shown in Figure 2-225.

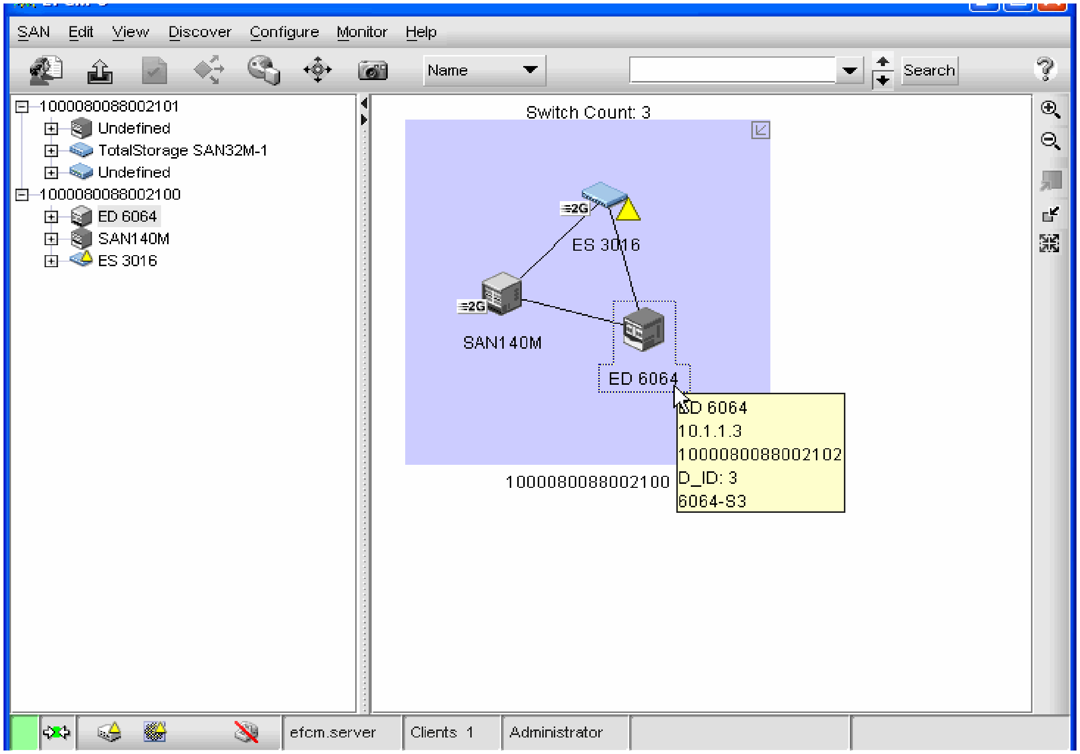

SAN
Edit
View
Discover
Configure
Monitor
Help
Name
Search
1000080088002101
Undefined
TotalStorage SAN32M-1
Undefined
1000080088002100
ED 6064
SAN140M
ES 3016
Switch Count: 3
2G
ES 3016
2G
SAN140M
ED 6064
1000080088002100
ED 6064
10.1.1.3
1000080088002102
D_ID: 3
6064-S3
efcm.server
Clients 1
Administrator

Figure 2-225 Product icon changed to normal state

Similarly, the bad power supply and fan units on the ES-3016 are also replaced to restore the switch status from degraded to normal operation.

2.23.3 Performing data collection

If a problem occurs that requires a support call to be raised, then the following data is required:

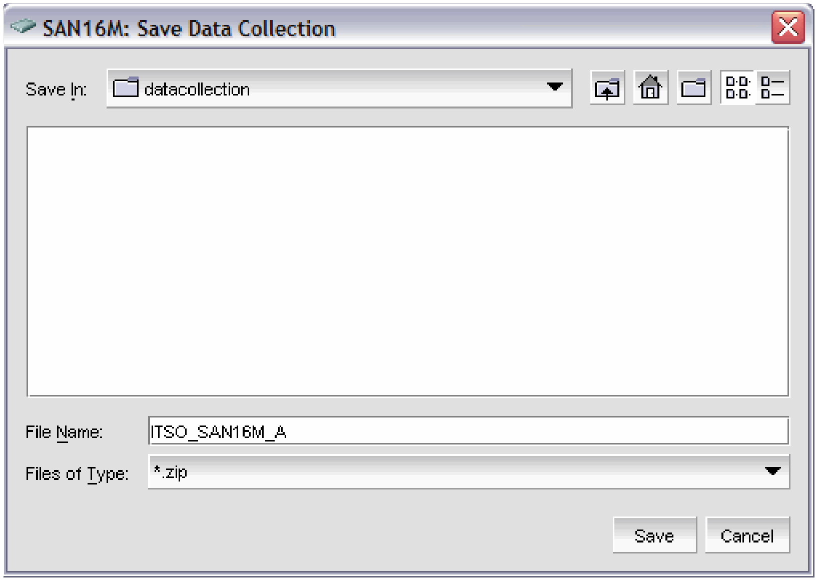
- Data collection from the affected switch, or all affected switches
- Detailed problem description
- Detailed SAN fabric diagram
- All ports involved with the problem and which HBAs or storage devices are connected to these ports
- Any relevant host error log information

All relevant information should be captured and sent to IBM support.

Data collection is done by selecting **Maintenance** → **Data Collection...** from the Element Manager.

Select a location to store the file, provide a suitable name, ensure that the file type is `.zip`, and click **Save**, as shown in Figure 2-226.

Note: The zip file is stored on the local machine running the EFCM client, and not on the EFCM server.

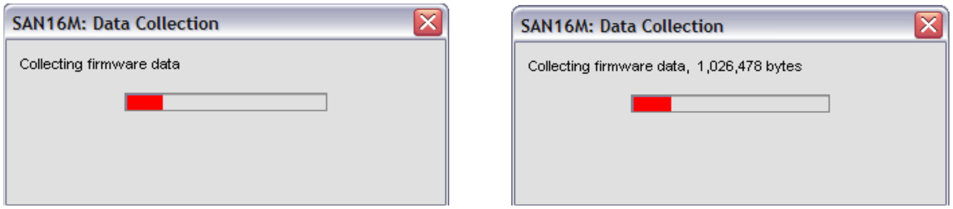


File Name: ITSO_SAN16M_A

Files of Type: *.zip

Figure 2-226   Data collection file specification

A progress bar displays, as shown in Figure 2-227, indicating the information being collected.



SAN16M: Data Collection
SAN16M: Data Collection

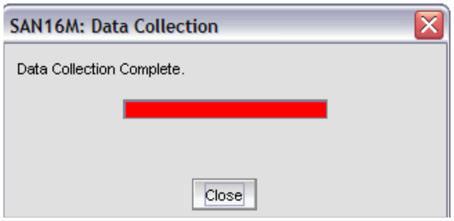
Collecting firmware data

Collecting firmware data, 1,026,478 bytes

Figure 2-227 Data collection progress

Tip: Data collections can take several minutes to complete.

On completion, you see the message in Figure 2-228 and should click **Close**.

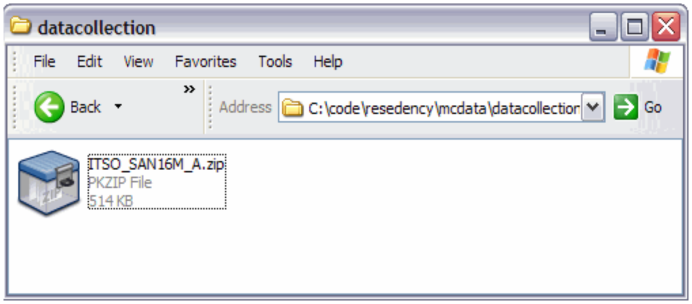


SAN16M: Data Collection
Close

Data Collection Complete.

Figure 2-228 Data collection complete

When data collection is completed, you have a zip file, shown in Figure 2-229, on the workstation from which you initiated the collection.



datacollection
File
Edit
View
Favorites
Tools
Help
Back
Address
Go

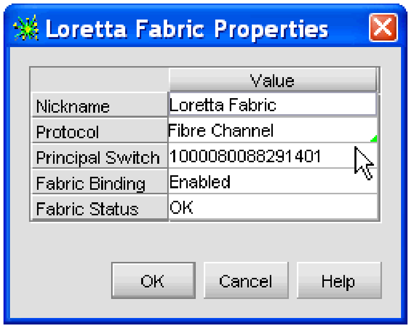
Address: C:\code\resedency\mcdata\datacollection

ITSO_SAN16M_A.zip
PKZIP File
514 KB

Figure 2-229 Zipped file from data collection

2.23.4 Identifying the principal switch

Sometimes you have to know which switch is acting as the principal switch. This can be determined with the **`show fabric principal`** CLI command, or by right-clicking the fabric in the EFCM and selecting **Properties**, which produces a display similar to Figure 2-230.



	Value
Nickname	Loretta Fabric
Protocol	Fibre Channel
Principal Switch	1000080088291401
Fabric Binding	Enabled
Fabric Status	OK

Figure 2-230 Determining fabric principal switch from EFCM

In both cases, the WWN of the principal switch is shown.

2.23.5 Performing a port wrap test

If errors are being reported on a link, or you suspect a switch port optic of having failed, then the switch port can be tested by inserting a wrap plug like that shown in Figure 2-231 and performing port diagnostics.

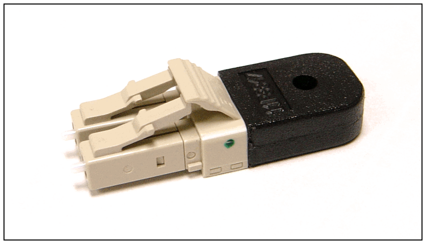
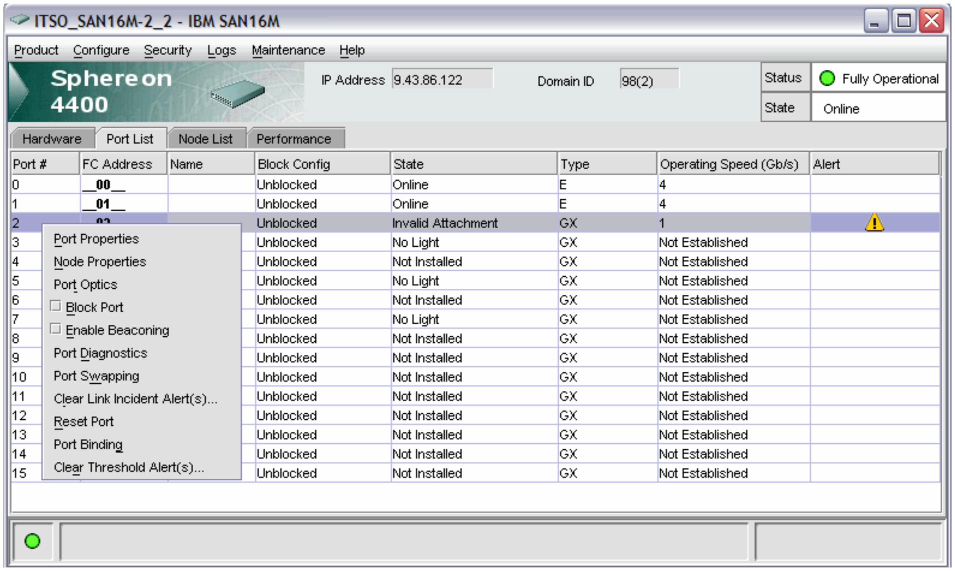


Figure 2-231 LC wrap plug

Launch the Element Manager and select the Port List tab. Now right-click against the port and select **Port(s) Diagnostics...** from the pop-up menu, as shown in Figure 2-232.


ITSO_SAN16M-2_2 - IBM SAN16M
Product Configure Security Logs Maintenance Help
Sphereon 4400
Hardware
Port List
Node List
Performance
Port Properties
Node Properties
Port Optics
☐ Block Port
☐ Enable Beaconing
Port Diagnostics
Port Swapping
Clear Link Incident Alert(s)...
Reset Port
Port Binding
Clear Threshold Alert(s)...

IP Address 9.43.86.122

Domain ID 98(2)

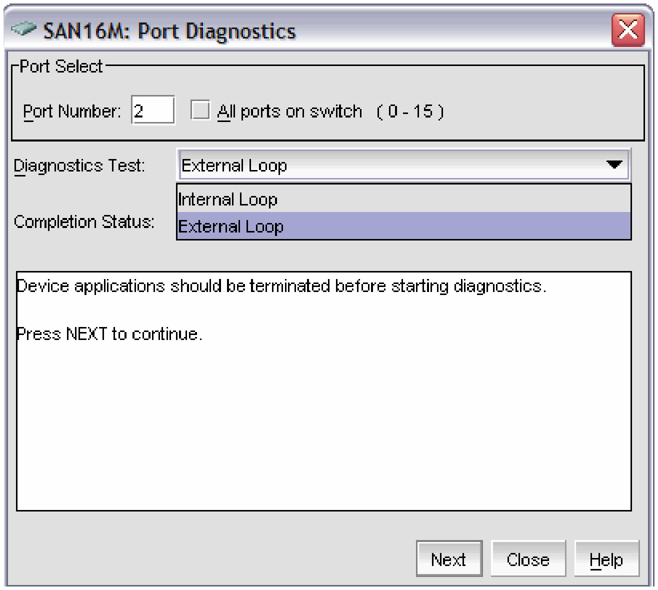
Status: Fully Operational

State: Online

Port #	FC Address	Name	Block Config	State	Type	Operating Speed (Gb/s)	Alert
0	__00__		Unblocked	Online	E	4	
1	__01__		Unblocked	Online	E	4	
2			Unblocked	Invalid Attachment	GX	1	⚠
3			Unblocked	No Light	GX	Not Established	
4			Unblocked	Not Installed	GX	Not Established	
5			Unblocked	No Light	GX	Not Established	
6			Unblocked	Not Installed	GX	Not Established	
7			Unblocked	No Light	GX	Not Established	
8			Unblocked	Not Installed	GX	Not Established	
9			Unblocked	Not Installed	GX	Not Established	
10			Unblocked	Not Installed	GX	Not Established	
11			Unblocked	Not Installed	GX	Not Established	
12			Unblocked	Not Installed	GX	Not Established	
13			Unblocked	Not Installed	GX	Not Established	
14			Unblocked	Not Installed	GX	Not Established	
15			Unblocked	Not Installed	GX	Not Established	

Figure 2-232 External wrap test port diagnostics step 1

Confirm that the correct Port Number is shown, change the Diagnostics Test from *Internal Loop* to *External Loop*, as shown in Figure 2-233, and click **Next**.


SAN16M: Port Diagnostics
Port Select
Internal Loop
External Loop
Next
Close
Help

Port Number: 2 ☐ All ports on switch (0 - 15)

Diagnostics Test: External Loop

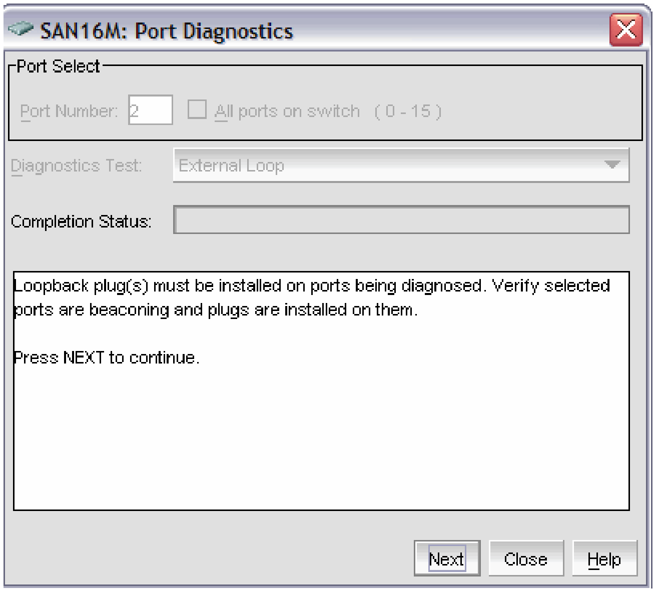
Completion Status:

Device applications should be terminated before starting diagnostics.

Press NEXT to continue.

Figure 2-233 External wrap test port diagnostics step 2

Verify the correct port by ensuring that the LED by the port is flashing. When the wrap plug is installed, click **Next** from the prompt in Figure 2-234.

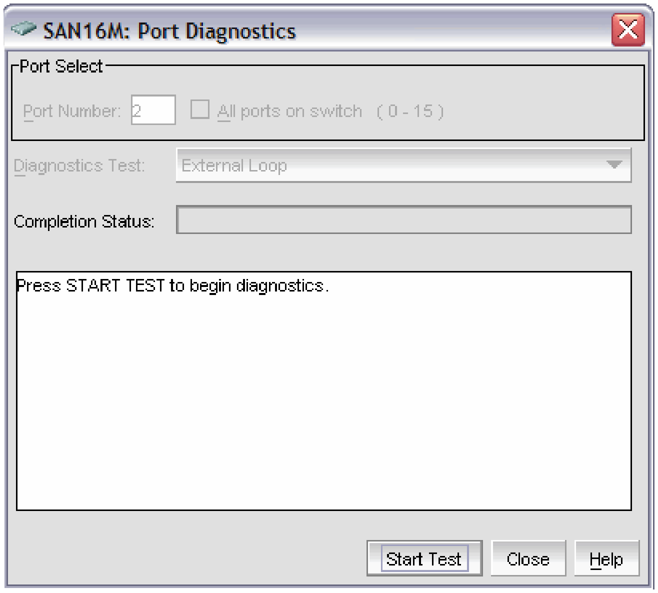

SAN16M: Port Diagnostics
Port Select
Port Number: 2
☐ All ports on switch (0 - 15)
Diagnostics Test: External Loop
Completion Status:
Next
Close
Help

Loopback plug(s) must be installed on ports being diagnosed. Verify selected ports are beaconing and plugs are installed on them.

Press NEXT to continue.

Figure 2-234 External wrap test port diagnostics step 3

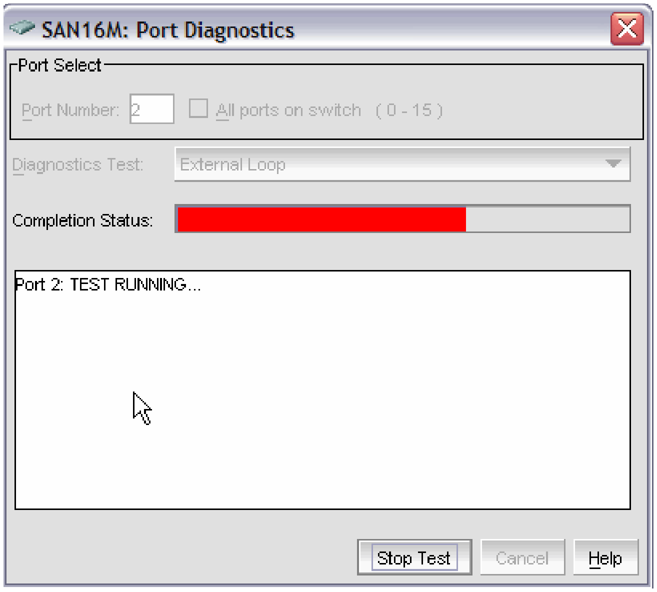
The test is now ready to start, so click **Start Test** as shown in Figure 2-235.


SAN16M: Port Diagnostics
Port Select
Port Number: 2
☐ All ports on switch (0 - 15)
Diagnostics Test: External Loop
Completion Status:
Start Test
Close
Help

Press START TEST to begin diagnostics.

Figure 2-235 External wrap test port diagnostics step 4

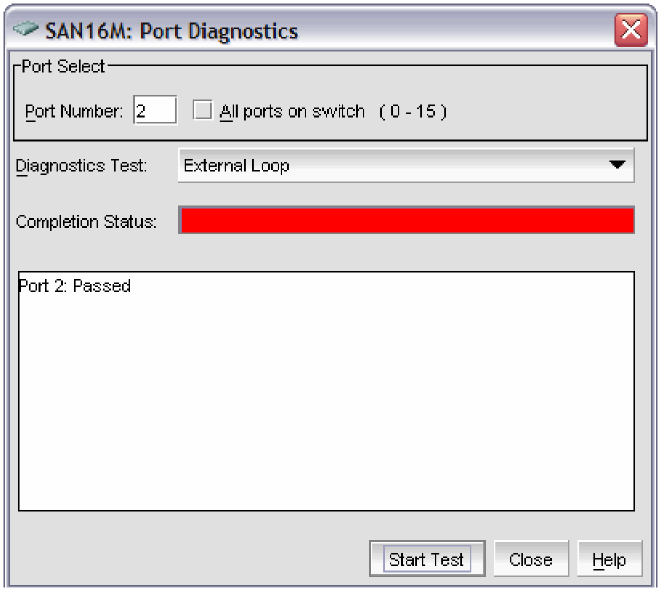
A progress bar displays, as shown in Figure 2-236, and the test takes about 30 seconds.


SAN16M: Port Diagnostics
Port Select
Port Number: 2
☐ All ports on switch (0 - 15)
Diagnostics Test: External Loop
Completion Status:
Stop Test
Cancel
Help

Port 2: TEST RUNNING...

Figure 2-236 External wrap test port diagnostics step 5

On successful completion, you should see the message in Figure 2-237.


SAN16M: Port Diagnostics
Port Select
All ports on switch (0 - 15)
Start Test
Close
Help

Port Number: 2

☐ All ports on switch (0 - 15)

Diagnostics Test: External Loop

Completion Status: 🟥

Port 2: Passed

Figure 2-237 External wrap test port diagnostics step 6

If the test fails, try swapping the SFP optic with a spare one and repeat the test to confirm the optic is faulty. If the test is now successful, then you should replace the original SFP with a new one.

Note: If call-home is enabled on the EFCM server and the wrap test fails, the server raises a call. It is advisable to temporarily disable call-home when performing wrap tests to avoid unwanted calls being generated.

2.23.6 Performing a cable wrap test

The same technique used to wrap test a switch port can be used to wrap test an installed fiber optic link. Simply attach the wrap plug at the remote end of the link using an LC-LC connector like that shown in Figure 2-238 and perform a normal external loop test.

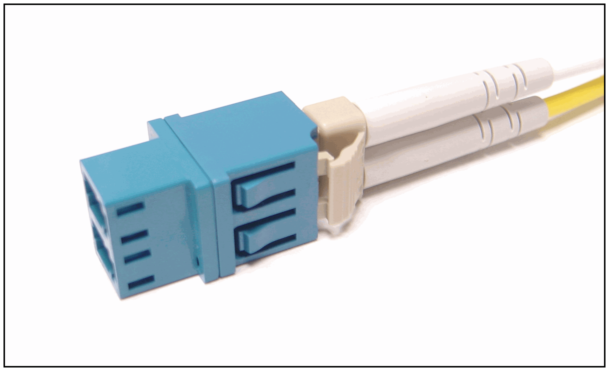


Figure 2-238 LC-LC connector attached to LC plug

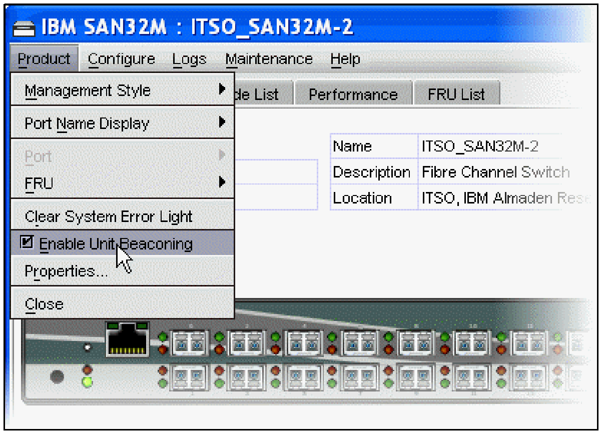
2.23.7 Testing a new fiber

If the fiber has not yet been installed, both ends are available to be connected to spare ports on the same switch. Ensure both ports are unblocked, and if the green LED next to each port lights, you know the fiber is good.

2.23.8 Unit beaconing

In a multi-switch environment, it is essential that you are able to identify the correct device in order to perform maintenance. As well as clearly labelling all switches and directors, it is possible to cause the system error LED to flash, or beacon, on the front left of the switch.

This is done by selecting **Product** → **Enable Unit Beaconing** as shown in Figure 2-239, which causes the yellow LED above the green power LED to flash, as illustrated in Figure 2-240.


IBM SAN32M : ITSO_SAN32M-2
Product
Configure
Logs
Maintenance
Help
Management Style
Port Name Display
Port
FRU
Clear System Error Light
☑ Enable Unit Beaconing
Properties...
Close
de List
Performance
FRU List

Name ITSO_SAN32M-2
Description Fibre Channel Switch
Location ITSO, IBM Almaden Res

Figure 2-239 Triggering unit beaconing

To disable the beaconing, repeat the **Product** → **Enable Unit Beaconing** steps.

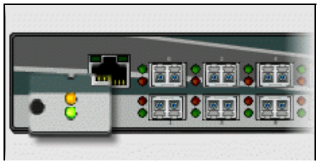


Figure 2-240 System error light

Note: For directors, the power and error lights are on the front top bezel.

Restriction: Beaconing is only possible if the system error light is not already lit due to an error.

2.23.9 Clearing the system error light

The system error LED shown in Figure 2-240 illuminates for problems such as power, fan, or port failures. Details of the failure can be seen in the Event Log, and the indicator remains lit until it is cleared.

To clear the error light, select **Product** → **Clear System Error Light**, as shown in Figure 2-239.

2.23.10 Port beaconing

As with unit beaconing, it is possible to beacon the LED next to a single port. This is achieved by right-clicking the port and selecting **Enable Beaconing** from the pop-up menu.

To disable the beaconing, repeat the procedure.

2.23.11 Detecting light in a fibre

A basic requirement when performing problem determination on a fiber link is being able to detect the presence or absence of light.

> **Warning:** We strongly recommend that you do *not* look directly at the end of a fiber to determine the presence of light, since this could cause eye damage. Furthermore, this does not work for longwave light, since it is infrared and hence is not visible to the eye. Instead you should use some form of light detector, such as a laser detection card, which utilizes phosphor to safely indicate the presence of light.

2.23.12 Fibre Channel trace route

The Telnet CLI provides a **`show fabric traceroute`** command which displays the route between two nodes in a fabric. It sends a frame through the fabric and shows the route taken to reach the destination and return to the source. It requires a source and destination port in either port ID or WWN format.

Refer to the *McDATA E/OS Command Line Interface User Manual*, 620-000134, for full details of the command output.

2.23.13 Switch factory default reset

It there is a requirement to reset all settings on the switch to factory default setting, you can use the following methods to do this.

Use the following steps to reset the configuration parameters on the Switch to the default values, using Figure 2-241:

1. Set the Switch offline. by selecting **Maintenance** → **Online State**.
2. Select **Maintenance** → **Reset Configuration**.

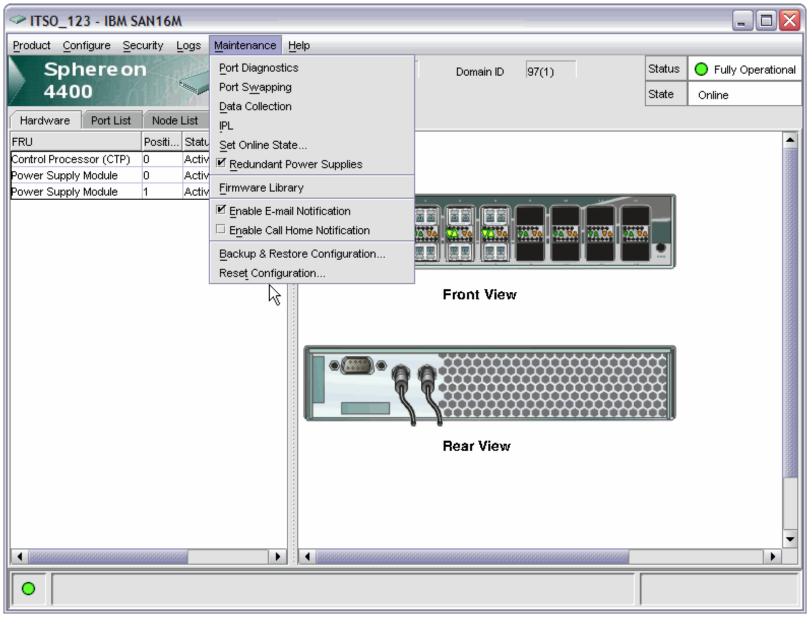
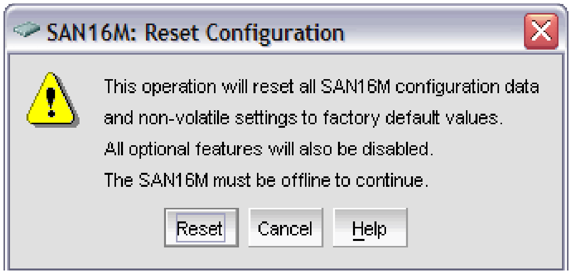

ITSO_123 - IBM SAN16M
Product Configure Security Logs Maintenance Help
Sphereon 4400
Hardware Port List Node List
FRU Positi... Statu
Control Processor (CTP) 0 Activ
Power Supply Module 0 Activ
Power Supply Module 1 Activ
Port Diagnostics
Port Swapping
Data Collection
IPL
Set Online State...
☑ Redundant Power Supplies
Firmware Library
☑ Enable E-mail Notification
☐ Enable Call Home Notification
Backup & Restore Configuration...
Reset Configuration...
Domain ID 97(1)
Status Fully Operational
State Online
Front View
Rear View

Figure 2-241 Reset to default

3. The warning message as shown in Figure 2-242 is displayed; read this and click **Reset** to continue.


SAN16M: Reset Configuration

This operation will reset all SAN16M configuration data and non-volatile settings to factory default values.

All optional features will also be disabled.

The SAN16M must be offline to continue.

Reset
Cancel
Help

Figure 2-242 Warning Message

Attention: Please note that since the internet protocol (IP) address resets to the factory default value during this procedure, you might not recover the Ethernet connection between the Switch and Server platform if you have changed the Switch IP addressing from that default value.

2.24 FICON quickstart configuration

In this topic we discuss the basic steps to configuring a switch for FICON in both a switched point-to-point and cascaded configuration.

We discuss some basic FICON/mainframe steps that you have to perform. It is not our intent to show any of the steps on the mainframe, however we highlight the considerations.

2.25 Hardware Configuration Definition

An I/O configuration defines the hardware resources available to the operating system and the connections between these resources. The resources include:

- Channels
- ESCON/FICON Directors (switches)
- Control units
- Devices

You must define an I/O configuration to the operating system (software) and the channel subsystem (hardware). The Hardware Configuration Definition (HCD) element of z/OS combines hardware and software I/O configuration under a single interactive end-user interface. HCD also performs validation checking, which helps to eliminate errors before you attempt to use the I/O configuration.

The output of HCD is an I/O definition file (IODF). An IODF is used to define multiple hardware and software configurations to the z/OS operating system. When you activate an IODF, HCD defines the I/O configuration to the channel subsystem and/or the operating system. With the HCD activate function or the `MVS ACTIVATE` operator command, you can make changes to the current configuration without having to perform an initial program load (IPL) the software or power-on reset (POR) the hardware. Making changes while the system is running is known as dynamic configuration or dynamic reconfiguration.

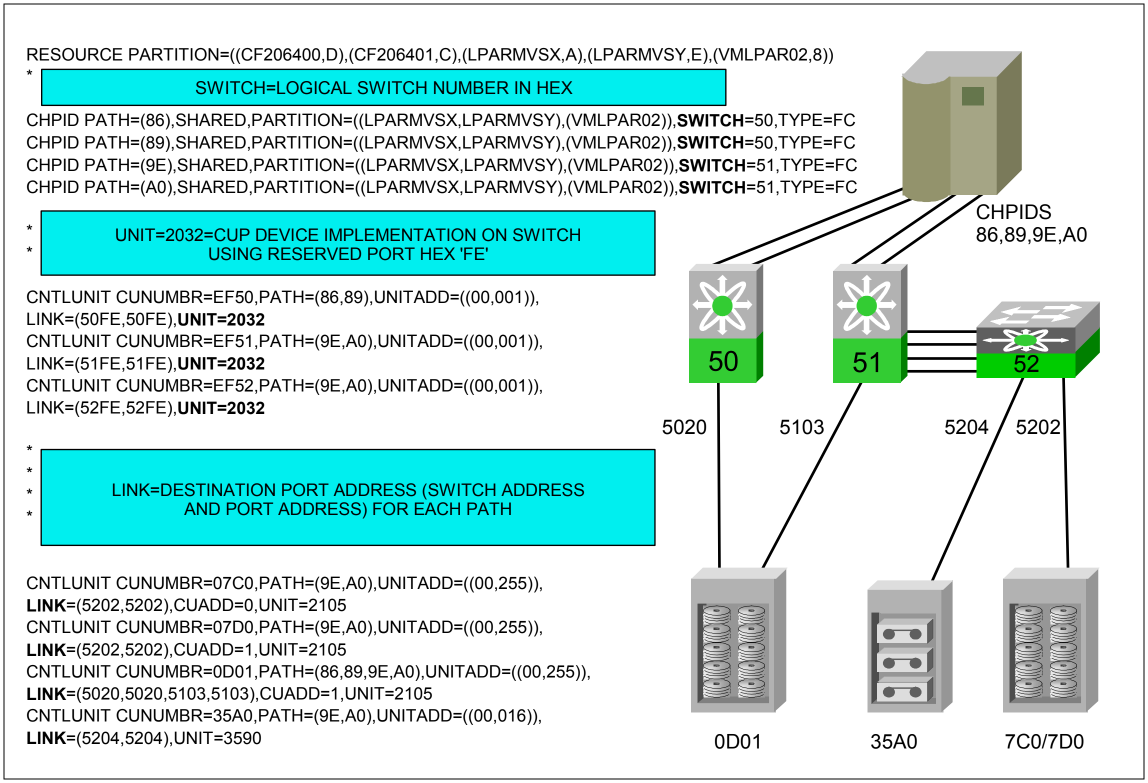
You select your I/O configuration when you:

- POR
- IPL
- Activate a dynamic configuration change

IPL and activation require that you identify the IODF that contains the definition of your configuration. A data set called an I/O configuration data set (IOCDS) is used at POR. An IOCDS can be created from a configuration definition in an IODF. The IOCDS contains the configuration for a specific processor, while the IODF contains configuration data for multiple processors.

> **Important:** We highly recommend that you complete the FICON configuration on the switches before attempting to bring any CHPIDs or Control Units online. Also, the switch configuration cannot be finished until HCD configuration is complete.

We show an example topology and associated statements in Figure 2-243.



```
RESOURCE PARTITION=((CF206400,D),(CF206401,C),(LPARMVSX,A),(LPARMVSY,E),(VMLPAR02,8))
*    SWITCH=LOGICAL SWITCH NUMBER IN HEX
CHPID PATH=(86),SHARED,PARTITION=((LPARMVSX,LPARMVSY),(VMLPAR02)),SWITCH=50,TYPE=FC
CHPID PATH=(89),SHARED,PARTITION=((LPARMVSX,LPARMVSY),(VMLPAR02)),SWITCH=50,TYPE=FC
CHPID PATH=(9E),SHARED,PARTITION=((LPARMVSX,LPARMVSY),(VMLPAR02)),SWITCH=51,TYPE=FC
CHPID PATH=(A0),SHARED,PARTITION=((LPARMVSX,LPARMVSY),(VMLPAR02)),SWITCH=51,TYPE=FC

*    UNIT=2032=CUP DEVICE IMPLEMENTATION ON SWITCH
*    USING RESERVED PORT HEX 'FE'

CNTLUNIT CUNUMBR=EF50,PATH=(86,89),UNITADD=((00,001)),
LINK=(50FE,50FE),UNIT=2032
CNTLUNIT CUNUMBR=EF51,PATH=(9E,A0),UNITADD=((00,001)),
LINK=(51FE,51FE),UNIT=2032
CNTLUNIT CUNUMBR=EF52,PATH=(9E,A0),UNITADD=((00,001)),
LINK=(52FE,52FE),UNIT=2032

*
*    LINK=DESTINATION PORT ADDRESS (SWITCH ADDRESS
*    AND PORT ADDRESS) FOR EACH PATH
*

CNTLUNIT CUNUMBR=07C0,PATH=(9E,A0),UNITADD=((00,255)),
LINK=(5202,5202),CUADD=0,UNIT=2105
CNTLUNIT CUNUMBR=07D0,PATH=(9E,A0),UNITADD=((00,255)),
LINK=(5202,5202),CUADD=1,UNIT=2105
CNTLUNIT CUNUMBR=0D01,PATH=(86,89,9E,A0),UNITADD=((00,255)),
LINK=(5020,5020,5103,5103),CUADD=1,UNIT=2105
CNTLUNIT CUNUMBR=35A0,PATH=(9E,A0),UNITADD=((00,016)),
LINK=(5204,5204),UNIT=3590
```

Figure 2-243 FICON environment IOCP definitions

> **Note:** There is no change to the IODEVICE or ID statements to support SAN.

We do not propose to cover the HCD definition process, because you must be familiar with that before attempting to code any of the statements shown in Figure 2-243.

For more information on FICON, we recommend the Redbooks publication, *FICON Implementation Guide*, SG24-6497, and refer you to:

`http://www.redbooks.ibm.com/abstracts/sg246497.html?Open`

2.25.1 McDATA FICON configuration consideration

IBM has developed a new machine type for FICON directors, 2027. However, all directors and switches, regardless of model or manufacture should be configured as 2032 (UNIT=2032).

Director/Switch Device Type

2032

Control Unit Port (CUP)

0xFE

Example: 4 CHPIDs (08,28,26, and 23) are defined for CUP:

```
CNTLUNIT CUNUMBR=0AD0,PATH=((CSS(0),08,28,26,23)), *
UNITADD=((00,001)),LINK=((CSS(0),FE,FE,FE,FE)),UNIT=2032
IODEVICE ADDRESS=AD0,UNITADD=00,CUNUMBR=(0AD0),STADET=Y, *
UNIT=2032
```

Note: When using the CUP port to frequently collect RMF™ statistics, we recommend that the primary path be dedicated for CUP functions only. Normally, a dedicated path is not used.

Switch ID and Switch Address

Switch Address = Domain ID (in hex) + 0x60

Example: Domain ID = 1; Switch Address = 0x61

Supported Range Of Switch Addresses: 0x61 – 0x7F

Always define the Switch ID to be the Switch Address. This avoid confusion when reviewing reports and alert messages.

Logical Port Number

Both physical and logical numbers are printed on the back of the directors and can be displayed on the management console.

Director/Switch Device Type

3232, 6064, and *6140

Port Number = Physical Port Number In Hex + 4

Note: Port numbers 0x84 through 0x87 are reserved for internal use only on the 6140 and cannot be used for external connections.

Example: CHPIDs 8 and 23 are to access DASD connected to the switch at ports 9 and 42 (0x09+4 = 0x0D and 0x2A+4 =0x2E)

```
CNTLUNIT CUNUMBR=0B00,PATH=((CSS(0),08,23)),*
UNITADD=((00,256)), *
LINK=((CSS(0),0D,2E)),CUADD=0, *
UNIT=2105
```

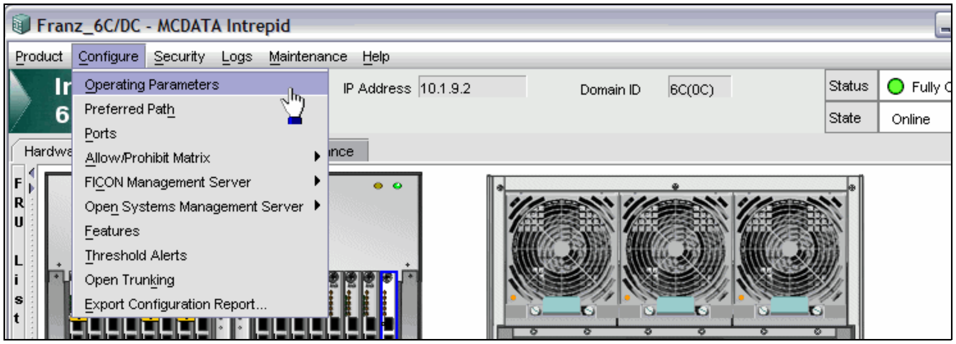
Director/Switch Device Type

i10K and 4700

There is no offset. Just make sure that you are using the hexadecimal equivalent of the port number.

2.26 Setting up the switch identification

To set up the switch identification, open the element manager for the switch as shown in Figure 2-244.


Franz_6C/DC - MCDATA Intrepid
Product
Configure
Security
Logs
Maintenance
Help
Operating Parameters
Preferred Path
Ports
Allow/Prohibit Matrix
FICON Management Server
Open Systems Management Server
Features
Threshold Alerts
Open Trunking
Export Configuration Report...
Hardwa
FRU List

IP Address 10.1.9.2

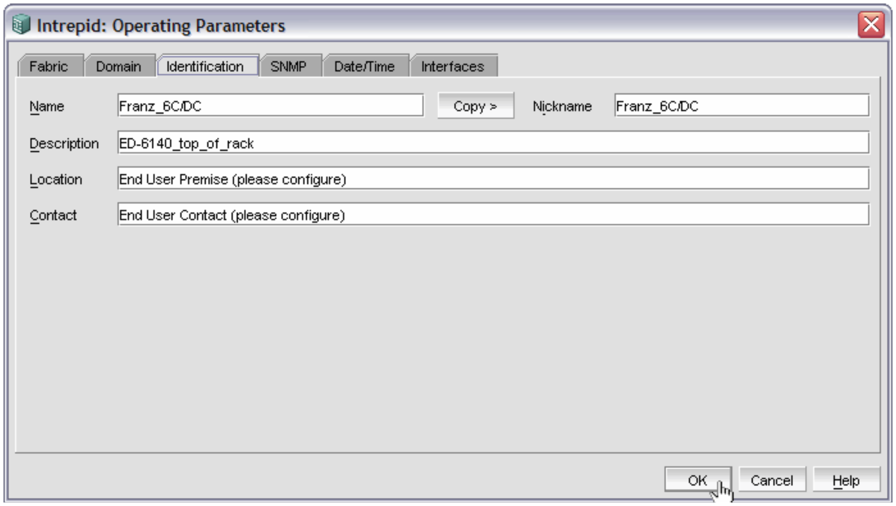
Domain ID 6C(0C)

Status Fully C

State Online

Figure 2-244 Configure Identification

Select the **Identification** tab from the pop-up menu shown in Figure 2-245, and fill in the blanks.


Intrepid: Operating Parameters
Fabric
Domain
Identification
SNMP
Date/Time
Interfaces
Copy >
OK
Cancel
Help

Name: Franz_6C/DC
Nickname: Franz_6C/DC
Description: ED-6140_top_of_rack
Location: End User Premise (please configure)
Contact: End User Contact (please configure)

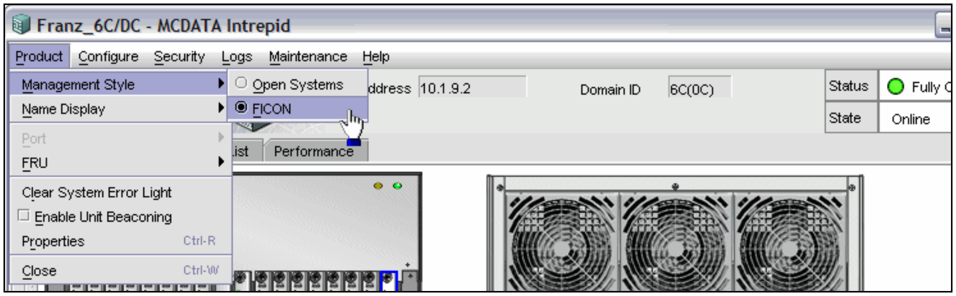
Figure 2-245 Identification

Click **OK** when done.

2.26.1 Setting the FICON view

This option might not be available in some EFCM versions, and in that case it is not necessary.

Setting the view to FICON management style allows you to use the prohibit/allow matrix and displays the logical port numbers in the port and node list displays. From the element manager, select **FICON** as shown in Figure 2-246.


Franz_6C/DC - MCDATA Intrepid
Product
Configure
Security
Logs
Maintenance
Help
Management Style
Name Display
Port
FRU
Clear System Error Light
☐ Enable Unit Beaconing
Properties Ctrl-R
Close Ctrl-W
ist
Performance

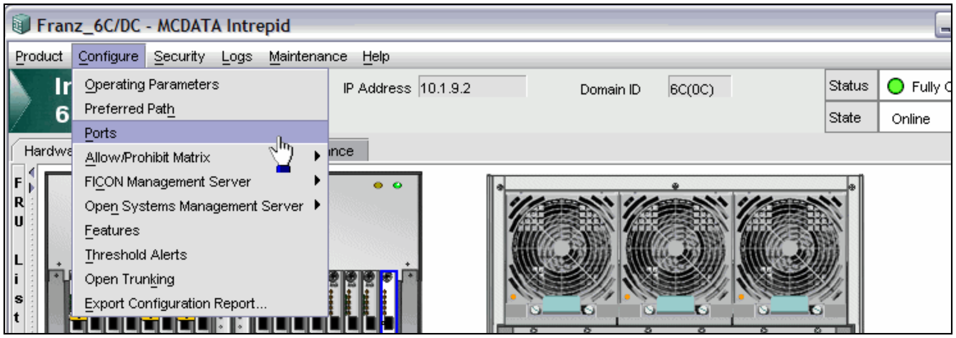
Management Style: ○ Open Systems ● FICON
ddress 10.1.9.2
Domain ID 6C(0C)
Status Fully
State Online

Figure 2-246 FICON view

2.26.2 Naming the ports

There is typically no requirement to name FICON ports, but it can be useful to name the ports where network equipment is connected in cascaded environments. In older versions of EFCM, you cannot name ports in the FICON management style view; however, any names you assign to ports while in the Open Systems management style are displayed when in FICON management style. You can flip back and forth between Open Systems and FICON management styles without effecting traffic in the director.

To name a port, from the element manager, select **Configure** →**Ports** as shown in Figure 2-247.



IP Address 10.1.9.2

Domain ID 6C(0C)

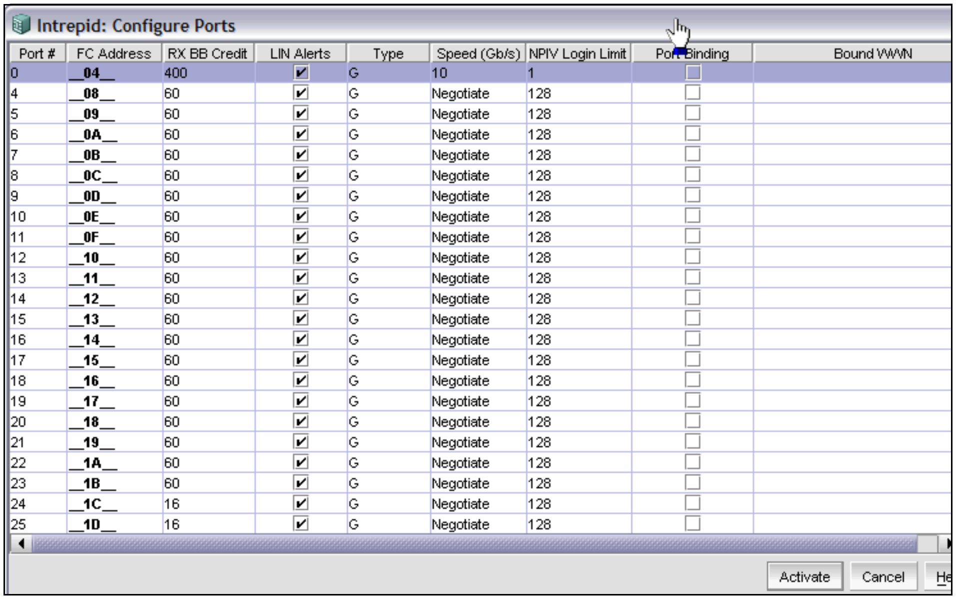
Status Fully C

State Online

Franz_6C/DC - MCDATA Intrepid
Product
Configure
Security
Logs
Maintenance
Help
Operating Parameters
Preferred Path
Ports
Allow/Prohibit Matrix
FICON Management Server
Open Systems Management Server
Features
Threshold Alerts
Open Trunking
Export Configuration Report...
Hardwa
nce
FRU List

Figure 2-247 Configure ports

Figure 2-248 shows the pop-up menu that displays on a FICON director.



Port #	FC Address	RX BB Credit	LIN Alerts	Type	Speed (Gb/s)	NPIV Login Limit	Port Binding	Bound WWN
0	__04__	400	☑	G	10	1	☐	
4	__08__	60	☑	G	Negotiate	128	☐	
5	__09__	60	☑	G	Negotiate	128	☐	
6	__0A__	60	☑	G	Negotiate	128	☐	
7	__0B__	60	☑	G	Negotiate	128	☐	
8	__0C__	60	☑	G	Negotiate	128	☐	
9	__0D__	60	☑	G	Negotiate	128	☐	
10	__0E__	60	☑	G	Negotiate	128	☐	
11	__0F__	60	☑	G	Negotiate	128	☐	
12	__10__	60	☑	G	Negotiate	128	☐	
13	__11__	60	☑	G	Negotiate	128	☐	
14	__12__	60	☑	G	Negotiate	128	☐	
15	__13__	60	☑	G	Negotiate	128	☐	
16	__14__	60	☑	G	Negotiate	128	☐	
17	__15__	60	☑	G	Negotiate	128	☐	
18	__16__	60	☑	G	Negotiate	128	☐	
19	__17__	60	☑	G	Negotiate	128	☐	
20	__18__	60	☑	G	Negotiate	128	☐	
21	__19__	60	☑	G	Negotiate	128	☐	
22	__1A__	60	☑	G	Negotiate	128	☐	
23	__1B__	60	☑	G	Negotiate	128	☐	
24	__1C__	16	☑	G	Negotiate	128	☐	
25	__1D__	16	☑	G	Negotiate	128	☐	

Figure 2-248   FICON ports

2.26.3 Validating features and installing FICON CUP Zoning

To validate features, and to install and activate the FICON CUP Zoning (FCZ) optional feature key, proceed as follows.

Open the Element Manager for the switch/director as shown in Figure 2-249.

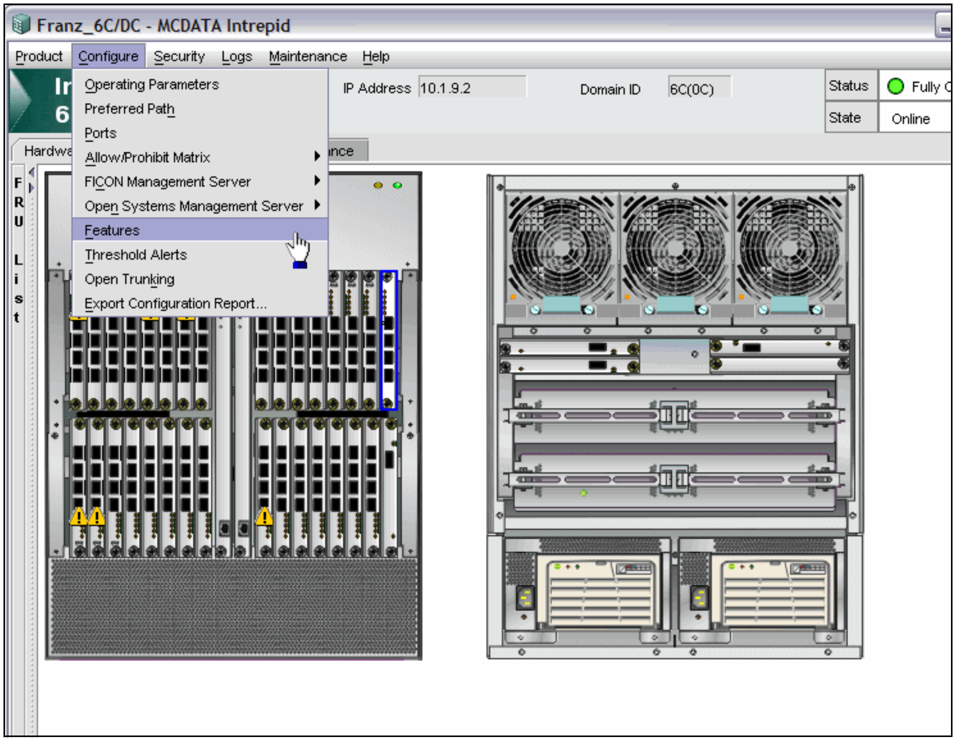
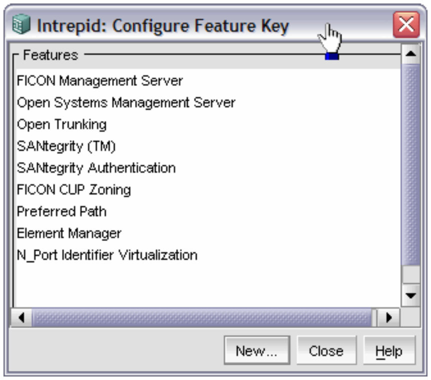

Franz_6C/DC - MCDATA Intrepid
Product
Configure
Security
Logs
Maintenance
Help
Operating Parameters
Preferred Path
Ports
Allow/Prohibit Matrix
FICON Management Server
Open Systems Management Server
Features
Threshold Alerts
Open Trunking
Export Configuration Report...
IP Address
10.1.9.2
Domain ID
6C(0C)
Status
Fully
State
Online
Hardwa
nce
FRU List

Figure 2-249 Configure features

A list of the installed features is displayed. We currently have FICON CUP Zoning installed, as can be seen in Figure 2-250.

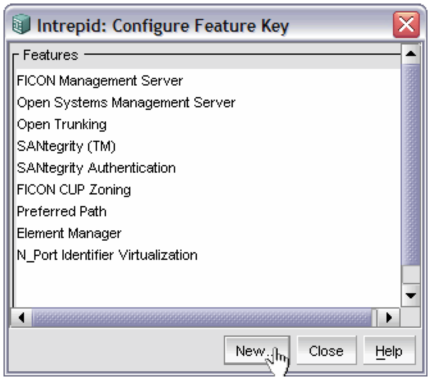
> **Note:** Obviously this same process can be used to identify the features that are currently enabled on the switch.


Intrepid: Configure Feature Key
Features
New...
Close
Help

FICON Management Server
Open Systems Management Server
Open Trunking
SANtegrity (TM)
SANtegrity Authentication
FICON CUP Zoning
Preferred Path
Element Manager
N_Port Identifier Virtualization

Figure 2-250 Features

Had it not already been installed, we would have clicked **New** as shown in Figure 2-251.


Intrepid: Configure Feature Key
Features
New...
Close
Help

FICON Management Server
Open Systems Management Server
Open Trunking
SANtegrity (TM)
SANtegrity Authentication
FICON CUP Zoning
Preferred Path
Element Manager
N_Port Identifier Virtualization

Figure 2-251 Add new feature

We would then have added the FICON CUP Zoning feature key code as shown in Figure 2-252.

> **Important:** Feature keys are not *added*. Every time you enter a feature key, it removes any features from the previous key and adds all features specified in the new key. Make sure that all the features you expect to have in the new key are present before entering the new key.

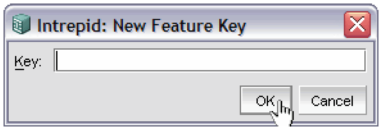

Intrepid: New Feature Key
Key:
OK
Cancel

Figure 2-252 New feature key

To uninstall the FICON CUP Zoning feature, enter a new key that does not contain the FICON CUP Zoning feature. Uninstalling FICON CUP Zoning requires the feature to be disabled.

2.26.4 Configuring switch parameters

From element manager, select **Configure** → **Operating Parameters** as shown in Figure 2-253.

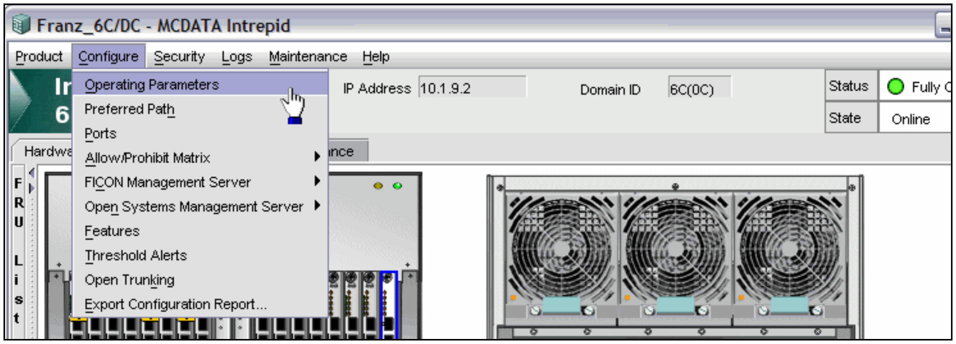
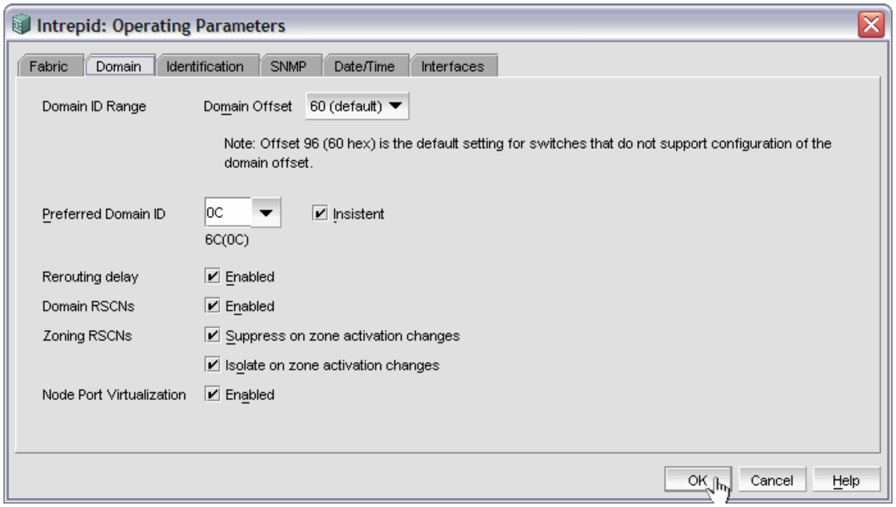

Franz_6C/DC - MCDATA Intrepid
Product
Configure
Security
Logs
Maintenance
Help
Operating Parameters
Preferred Path
Ports
Allow/Prohibit Matrix
FICON Management Server
Open Systems Management Server
Features
Threshold Alerts
Open Trunking
Export Configuration Report...
IP Address
10.1.9.2
Domain ID
6C(0C)
Status
Fully
State
Online
Hardwa
nce
FRU List

Figure 2-253 Configure operating parameters

Select the **Domain** tab as shown in Figure 2-254.


Intrepid: Operating Parameters
Fabric
Domain
Identification
SNMP
Date/Time
Interfaces
OK
Cancel
Help

Domain ID Range   Domain Offset 60 (default)

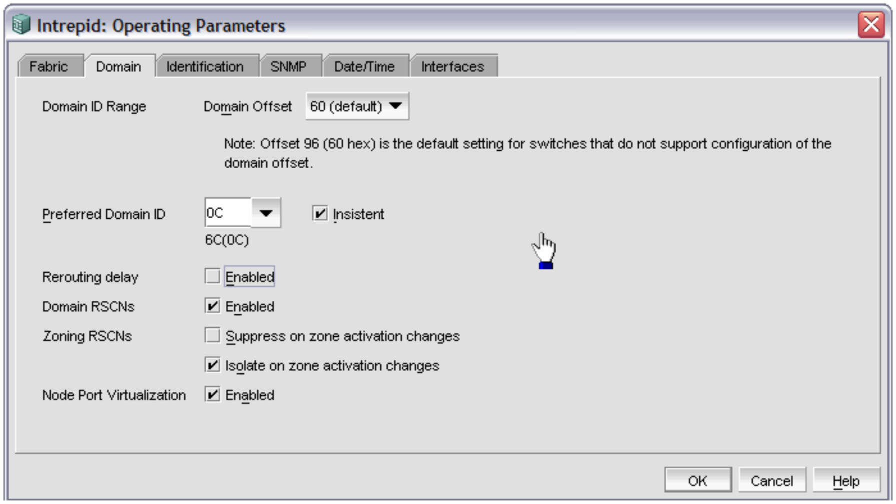
Note: Offset 96 (60 hex) is the default setting for switches that do not support configuration of the domain offset.

Preferred Domain ID 0C ☑ Insistent
6C(0C)

Rerouting delay ☑ Enabled
Domain RSCNs ☑ Enabled
Zoning RSCNs ☑ Suppress on zone activation changes
☑ Isolate on zone activation changes
Node Port Virtualization ☑ Enabled

Figure 2-254 Domain

For FICON we set the parameters as shown in Figure 2-255.


Intrepid: Operating Parameters
Fabric
Domain
Identification
SNMP
Date/Time
Interfaces
OK
Cancel
Help

Domain ID Range   Domain Offset 60 (default)

Note: Offset 96 (60 hex) is the default setting for switches that do not support configuration of the domain offset.

Preferred Domain ID 0C ☑ Insistent
6C(0C)

Rerouting delay ☐ Enabled
Domain RSCNs ☑ Enabled
Zoning RSCNs ☐ Suppress on zone activation changes
☑ Isolate on zone activation changes
Node Port Virtualization ☑ Enabled

Figure 2-255 FICON domain parameters

In cascaded FICON environments, the switch address (which is based on the Domain ID) is used in the I/O configuration and therefore setting the Domain ID to be both insistent and unique is required for two-byte addressing.

Tip: Although only required for two-byte addressing, setting the Domain ID to be insistent and unique is a recommended best practice for all FICON environments.

In Figure 2-255 on page 617 we can set the following parameters:

Domain ID Range: The domain identification (Domain ID) number is a unique identification for the switch in a fabric. A distinct ID is automatically allocated to each switch in the fabric by the principal switch. A switch cannot contain the same domain ID as another switch or their E_Ports will segment when they try to join as a fabric. The Domain ID Range options allow you to configure or expand the range of possible domain IDs in a fabric from the legacy McDATA range of 96-127 IDs.

Domain Offset: Selecting the Domain Offset option and value from the drop-down list, allows you to configure the domain offset values. Domain IDs minus the offset are still in the 1-31 range. Values available in the drop-down list are 0, 20, 40, 60, 80, A0, and C0. 60 is the default.

Preferred: Enter the desired domain ID in decimal (1-31) here. The switch address is the hexadecimal equivalent of the domain ID plus x’60’. In the example above, the Domain ID is 0C, so the switch address is 6C(0C).

Insistent: Checking the insistent box is required for cascading and recommended otherwise. Checking insistent forces the active domain ID to be the preferred domain ID.

Note: Changing the active domain ID is an offline function.

Rerouting Delay: Leave this unchecked (disabled).

Domain RSCNs: Domain RSCNs lets zSeries processors know whenever a switch enters or leaves the fabric. This information, however, serves no useful purpose. Furthermore, although control units do nothing with it, it does require some processing.

Zoning RSCNs: There are two choices here:

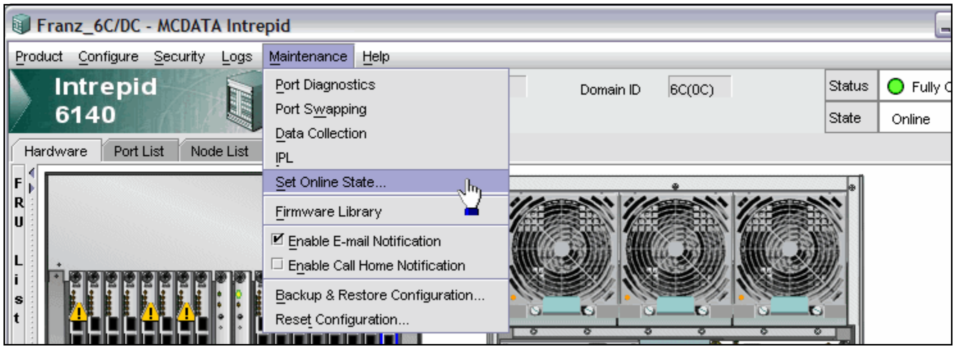
- Suppress on zone activation changes — This should be checked (negative logic here — checking the box *disables* zoning RSCNs).
- Isolate on zone activation changes — When selected, only devices that require RSCN notification for a zoning configuration change receive RSCNs. This option does not have to be selected if Suppress on zone activation changes is selected, since RSCNs are not sent to attached devices.

Node Port Virtualization: Only check this box if a channel that supports node port virtualization is to be attached. This feature allows you to assign multiple Fibre Channel addresses to a single N_Port. Enable this feature mainly for systems that support multiple images behind a single node port.

2.26.5 Setting the switch offline

Do not put the switch offline unless necessary. Changing some parameters can require the switch to be offline.

Setting a switch offline breaks all connections, so if this is necessary in a production environment, you have to plan to configure all CHPIDs offline that are either directly connected to the switch or are connected to control units connected to that switch. Select **Maintenance** → **Set Online State** as shown in Figure 2-256.


Franz_6C/DC - MCDATA Intrepid
Product
Configure
Security
Logs
Maintenance
Help
Intrepid 6140
Port Diagnostics
Port Swapping
Data Collection
IPL
Set Online State...
Firmware Library
☑ Enable E-mail Notification
☐ Enable Call Home Notification
Backup & Restore Configuration...
Reset Configuration...
Hardware
Port List
Node List
FRU List

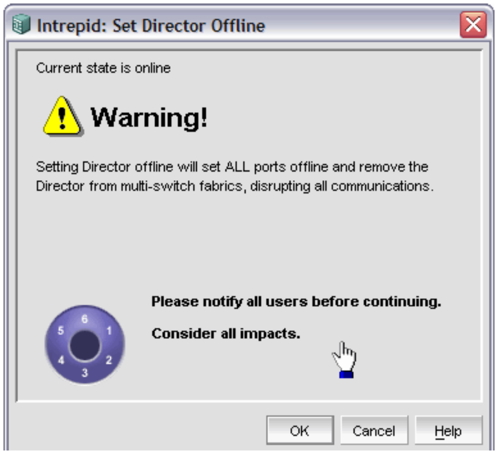
Domain ID 6C(0C)

Status Fully C

State Online

Figure 2-256 Set online state

You are presented with the warning window shown in Figure 2-257.



Current state is online

Warning!

Setting Director offline will set ALL ports offline and remove the Director from multi-switch fabrics, disrupting all communications.

Please notify all users before continuing.

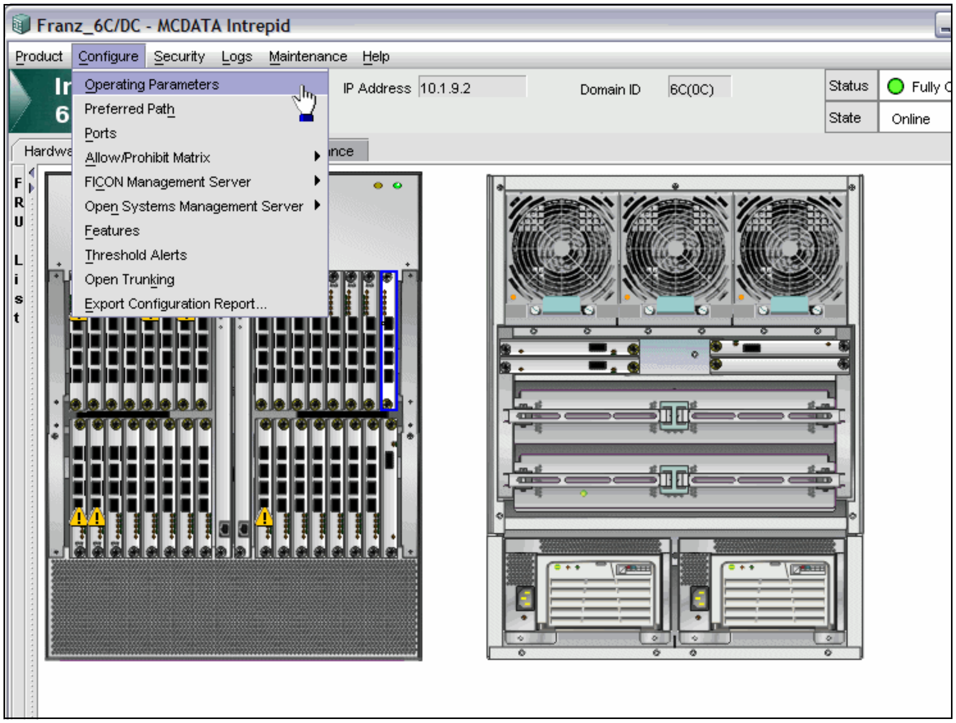
Consider all impacts.

Figure 2-257 Warning window

If you are certain, then click **OK**. Use the same process to set it online again.

2.26.6 Setting fabric parameters

We set the fabric parameters by selecting **Configure** → **Operating Parameters** as shown in Figure 2-258.


Franz_6C/DC - MCDATA Intrepid
Product
Configure
Security
Logs
Maintenance
Help
Operating Parameters
Preferred Path
Ports
Allow/Prohibit Matrix
FICON Management Server
Open Systems Management Server
Features
Threshold Alerts
Open Trunking
Export Configuration Report...
Hardwa
nce
F R U L i s t
Status
Fully
State

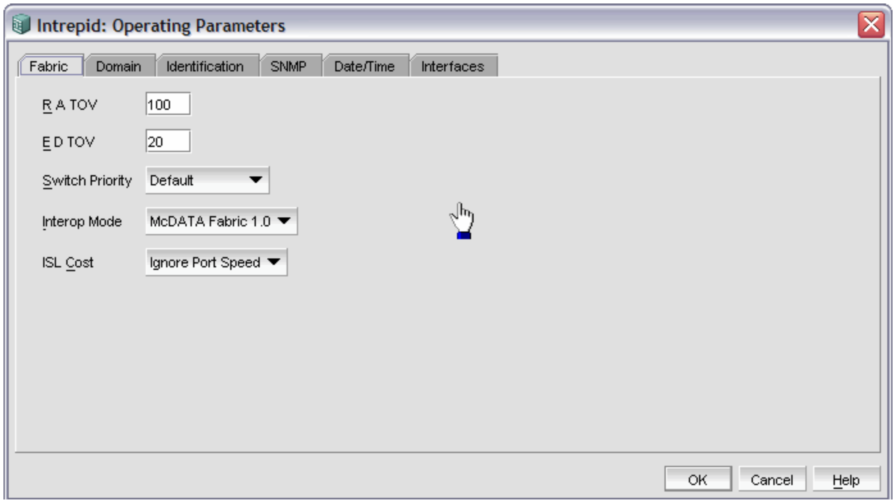
IP Address 10.1.9.2

Domain ID 6C(0C)

State Online

Figure 2-258 Fabric parameters

We click the **Fabric** tab as shown in Figure 2-259.


Intrepid: Operating Parameters
Fabric
Domain
Identification
SNMP
Date/Time
Interfaces
OK
Cancel
Help

R A TOV 100

E D TOV 20

Switch Priority Default

Interop Mode McDATA Fabric 1.0

ISL Cost Ignore Port Speed

Figure 2-259 Fabric tab

We set the following fabric parameters:

R_A_TOV — Resource_Allocation_Timeout Value: Unless advised otherwise by a qualified McDATA SAN specialist, leave at the factory default of 100.

E_D_TOV — Error Detect Timeout Value: The factory default of 20 should be used except when McDATA Edge 3000 equipment will be used with ISL links. A value of 50 should be used whenever Edge 3000 equipment is used.

Note: E_D_TOV must be the same on all cascaded directors. If some ISLs are connected with fiber, either direct or through DWDM, and some are connected with Edge 3000 equipment, the E_D_TOV must be set to 50 on all cascaded directors. This situation typically occurs when there is a near line hot backup site and another backup site in a different geographic area or there is a central backup hub serving some sites within fiber distance and others requiring long distance Telco extension.

Switch Priority: Do not change. In an open systems fabric, there is one principal switch that determines the domain IDs for all other switches in the event of a fabric rebuild. Since FICON cascading requires insistent domain IDs, there is never a requirement to dynamically assign domain IDs.

Interop Mode: McDATA Fabric mode should always be used in FICON environments. Open systems mode does not allow zoning by port number.

Note: Changing the Interop Mode is an offline function.

ISL Cost: There are two choices here:

- By Port Speed — Select if you want FSPF routing selection to account for port speed when assigning traffic to ISLs. Traffic skews to the higher speed ISL until it is at or near capacity, then it routes some traffic to the lower speed ISL.
- Ignore Port Speed — Select if you want FSPF routing selection to not account for port speed when assigning traffic to ISLs. All ISLs have equal cost.

2.26.7 Zoning

In the sequence of window captures that follow, we identify members of our FICON zone (for simplicity, we only choose three members). We create our FICON zone, create a zone set, place the zone in it, and show how to activate the zone set.

From element manager, select **Configure** →**Zoning** as shown in Figure 2-260.

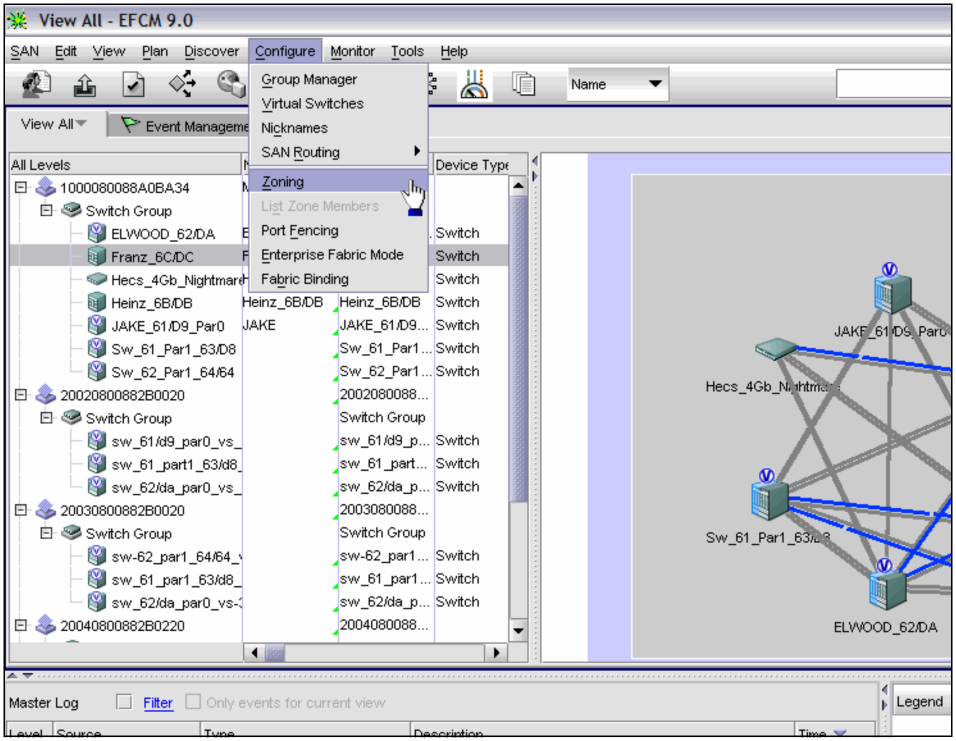
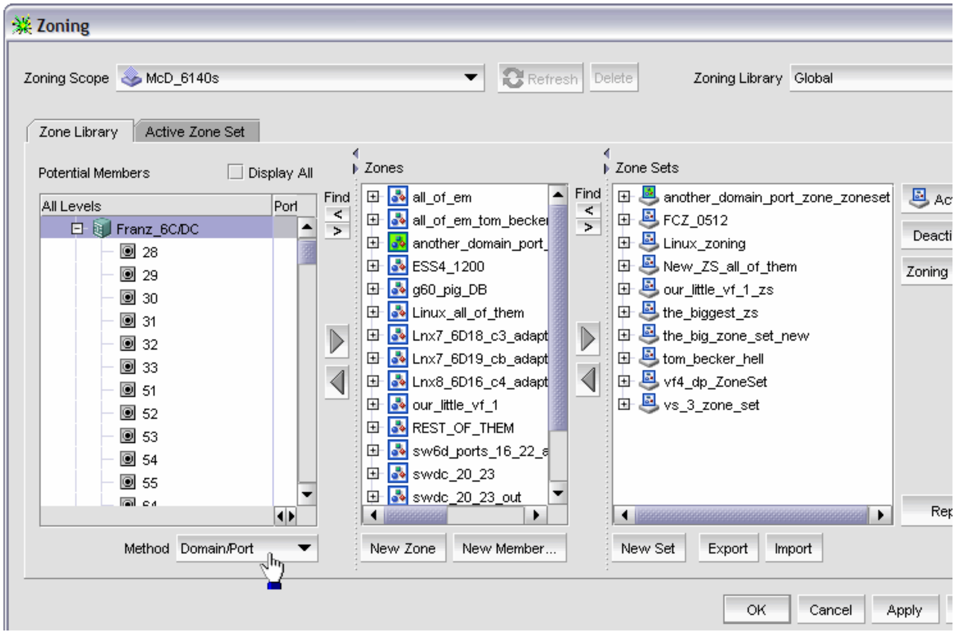

View All - EFCM 9.0
SAN Edit View Plan Discover Configure Monitor Tools Help
Group Manager
Virtual Switches
Nicknames
SAN Routing
Zoning
List Zone Members
Port Fencing
Enterprise Fabric Mode
Fabric Binding
Name
View All
Event Manageme
All Levels
Device Type
1000080088A0BA34
Switch Group
ELWOOD_62/DA
Franz_6C/DC
Hecs_4Gb_Nightmar
Heinz_6B/DB
JAKE_61/D9_Par0
Sw_61_Par1_63/D8
Sw_62_Par1_64/64
20020800882B0020
Switch Group
sw_61/d9_par0_vs_
sw_61_part1_63/d8_
sw_62/da_par0_vs_
20030800882B0020
Switch Group
sw-62_par1_64/64_
sw_61_par1_63/d8_
sw_62/da_par0_vs-
20040800882B0220
Switch
JAKE_61/D9_Par0
Hecs_4Gb_Nightmare
Sw_61_Par1_63/D8
ELWOOD_62/DA
Master Log
Filter
Only events for current view
Legend
Level Source Type Description Time

Figure 2-260 Configure zoning

From the Zone Library, we select our director and use **Domain/Port** as our method of zoning, as shown in Figure 2-261.



Zoning Scope: McD_6140s

Zoning Library: Global

Method: Domain/Port

Zoning
Refresh
Delete
Zone Library
Active Zone Set
Potential Members
Display All
All Levels
Port
Franz_6C/DC
28
29
30
31
32
33
51
52
53
54
55
Find
<
>
Zones
all_of_em
all_of_em_tom_becker
another_domain_port_
ESS4_1200
g60_pig_DB
Linux_all_of_them
Lnx7_6D18_c3_adapt
Lnx7_6D19_cb_adapt
Lnx8_6D16_c4_adapt
our_little_vf_1
REST_OF_THEM
sw6d_ports_16_22_
swdc_20_23
swdc_20_23_out
Zone Sets
another_domain_port_zone_zoneset
FCZ_0512
Linux_zoning
New_ZS_all_of_them
our_little_vf_1_zs
the_biggest_zs
the_big_zone_set_new
tom_becker_hell
vf4_dp_ZoneSet
vs_3_zone_set
Ac
Deacti
Zoning
Rep
New Zone
New Member...
New Set
Export
Import
OK
Cancel
Apply

Figure 2-261 Zone library and method

We click **New Zone** as shown in Figure 2-262.

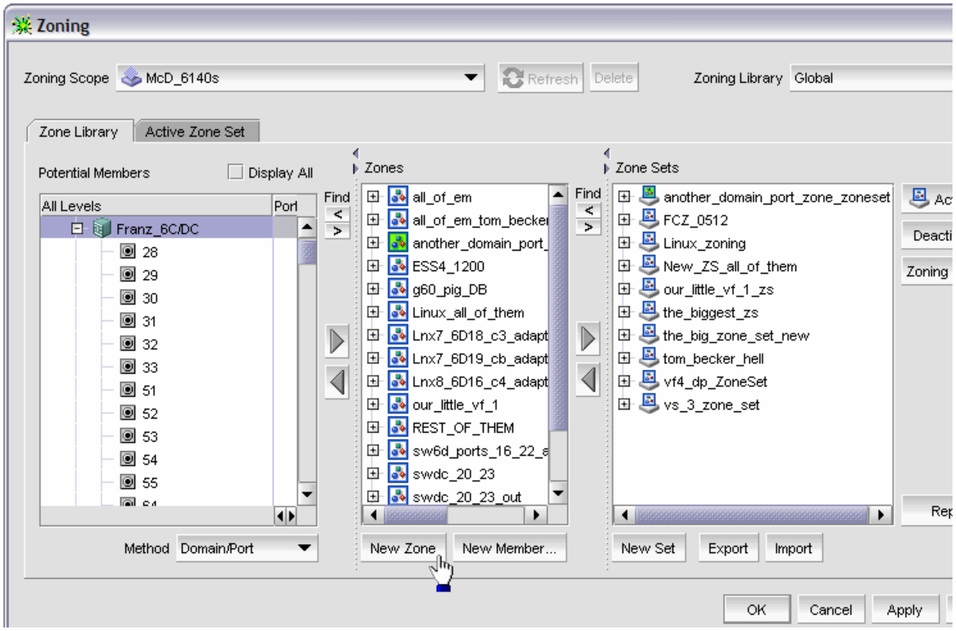
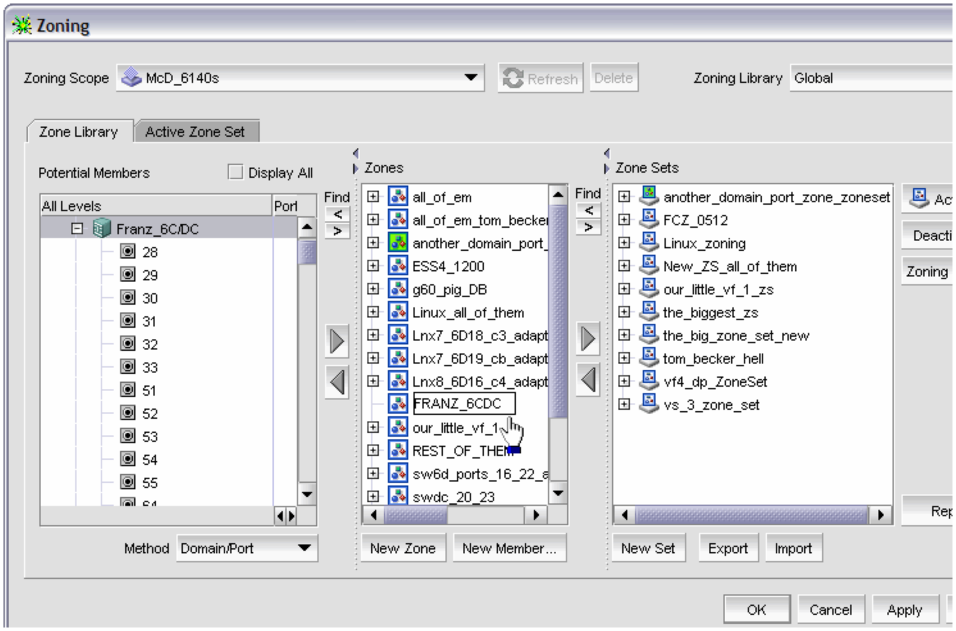

Zoning
Zoning Scope
McD_6140s
Refresh
Delete
Zoning Library
Global
Zone Library
Active Zone Set
Potential Members
Display All
All Levels
Port
Franz_6C/DC
28
29
30
31
32
33
51
52
53
54
55
Find
Zones
all_of_em
all_of_em_tom_becke
another_domain_port_
ESS4_1200
g60_pig_DB
Linux_all_of_them
Lnx7_6D18_c3_adapt
Lnx7_6D19_cb_adapt
Lnx8_6D16_c4_adapt
our_little_vf_1
REST_OF_THEM
sw6d_ports_16_22_
swdc_20_23
swdc_20_23_out
Zone Sets
another_domain_port_zone_zoneset
FCZ_0512
Linux_zoning
New_ZS_all_of_them
our_little_vf_1_zs
the_biggest_zs
the_big_zone_set_new
tom_becker_hell
vf4_dp_ZoneSet
vs_3_zone_set
Ac
Deacti
Zoning
Rep
Method
Domain/Port
New Zone
New Member...
New Set
Export
Import
OK
Cancel
Apply

Figure 2-262 New zone

We enter the name of our zone as shown in Figure 2-263.



Zoning Scope: McD_6140s

Zoning Library: Global

Method: Domain/Port

Zoning
Refresh
Delete
Zone Library
Active Zone Set
Potential Members
☐ Display All
All Levels
Port
Franz_6C/DC
28
29
30
31
32
33
51
52
53
54
55
Find
Zones
all_of_em
all_of_em_tom_becker
another_domain_port_
ESS4_1200
g60_pig_DB
Linux_all_of_them
Lnx7_6D18_c3_adapt
Lnx7_6D19_cb_adapt
Lnx8_6D16_c4_adapt
FRANZ_6CDC
our_little_vf_1
REST_OF_THEM
sw6d_ports_16_22_a
swdc_20_23
New Zone
New Member...
Find
Zone Sets
another_domain_port_zone_zoneset
FCZ_0512
Linux_zoning
New_ZS_all_of_them
our_little_vf_1_zs
the_biggest_zs
the_big_zone_set_new
tom_becker_hell
vf4_dp_ZoneSet
vs_3_zone_set
New Set
Export
Import
Ac
Deacti
Zoning
Rep
OK
Cancel
Apply

Figure 2-263 Naming new zone

When we have done this, we select the ports we want to put in the zone we just created. For the purposes of this example we are only selecting 3 ports. If this was our FICON environment, we would have put all FICON ports into this zone. We put the ports in the new zone by clicking the right arrow as shown in Figure 2-264.

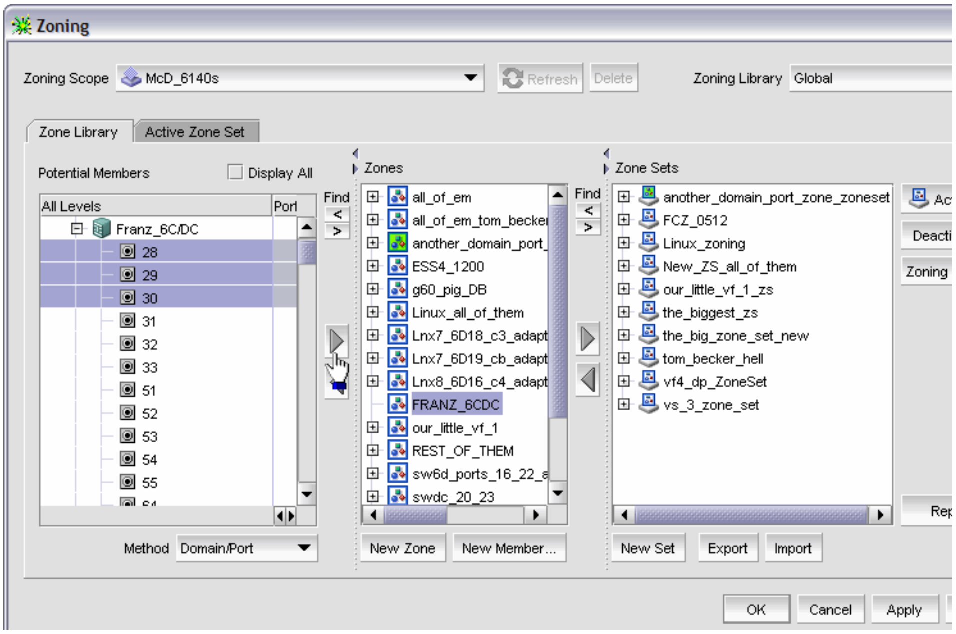

Zoning
Zoning Scope
McD_6140s
Refresh
Delete
Zoning Library
Global
Zone Library
Active Zone Set
Potential Members
Display All
All Levels
Port
Franz_6C/DC
28
29
30
31
32
33
51
52
53
54
55
Find
Method
Domain/Port
Zones
all_of_em
all_of_em_tom_becker
another_domain_port_
ESS4_1200
g60_pig_DB
Linux_all_of_them
Lnx7_6D18_c3_adapt
Lnx7_6D19_cb_adapt
Lnx8_6D16_c4_adapt
FRANZ_6CDC
our_little_vf_1
REST_OF_THEM
sw6d_ports_16_22_
swdc_20_23
New Zone
New Member...
Zone Sets
another_domain_port_zone_zoneset
FCZ_0512
Linux_zoning
New_ZS_all_of_them
our_little_vf_1_zs
the_biggest_zs
the_big_zone_set_new
tom_becker_hell
vf4_dp_ZoneSet
vs_3_zone_set
New Set
Export
Import
Deacti
Zoning
OK
Cancel
Apply

Figure 2-264 Moving ports to new zone

When this is done, we can see the new members in our zone as shown in Figure 2-265.

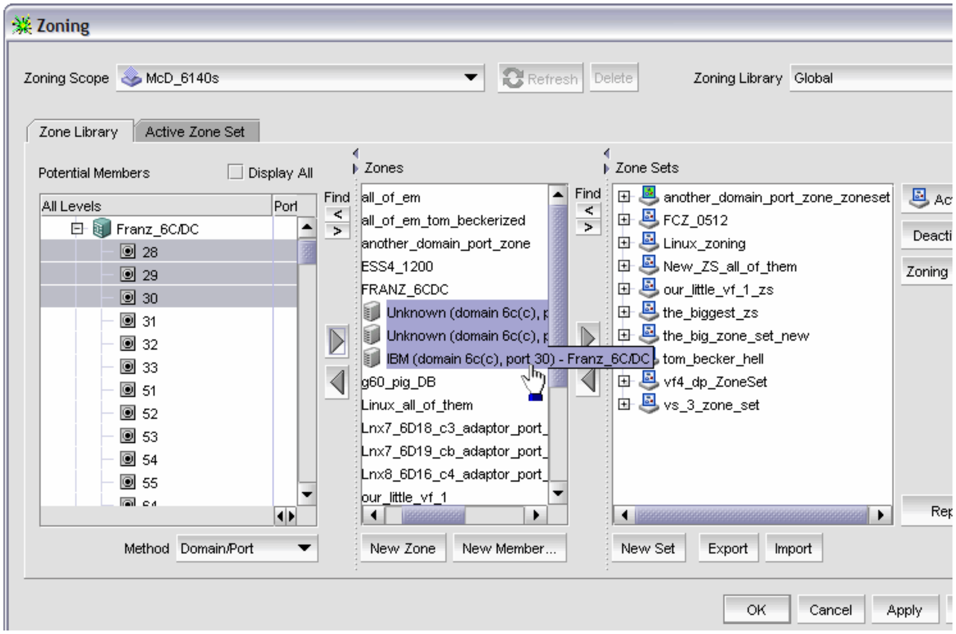

Zoning Scope: McD_6140s
Zoning Library: Global
Method: Domain/Port
☐ Display All
Zoning
Refresh
Delete
Zone Library
Active Zone Set
Potential Members
All Levels
Port
Franz_6C/DC
28
29
30
31
32
33
51
52
53
54
55
Find
<
>
Zones
all_of_em
all_of_em_tom_beckerized
another_domain_port_zone
ESS4_1200
FRANZ_6CDC
Unknown (domain 6c(c), p
Unknown (domain 6c(c), p
IBM (domain 6c(c), port 30) - Franz_6C/DC
g60_pig_DB
Linux_all_of_them
Lnx7_6D18_c3_adaptor_port_
Lnx7_6D19_cb_adaptor_port_
Lnx8_6D16_c4_adaptor_port_
our_little_vf_1
New Zone
New Member...
Zone Sets
another_domain_port_zone_zoneset
FCZ_0512
Linux_zoning
New_ZS_all_of_them
our_little_vf_1_zs
the_biggest_zs
the_big_zone_set_new
tom_becker_hell
vf4_dp_ZoneSet
vs_3_zone_set
New Set
Export
Import
Ac
Deacti
Zoning
Rep
OK
Cancel
Apply

Figure 2-265 New zone members added

Now we create a new zone set as shown in Figure 2-266.

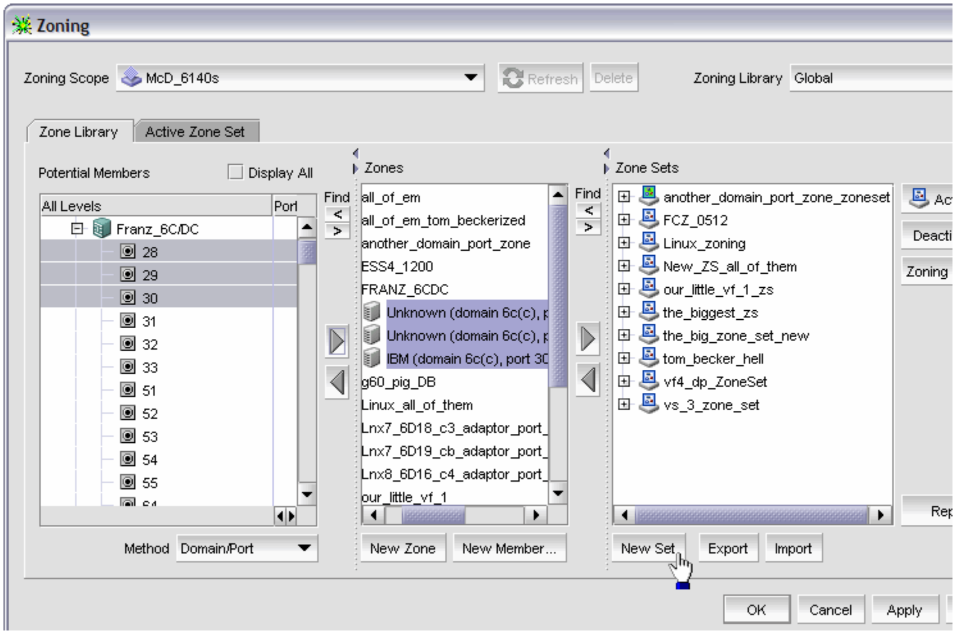
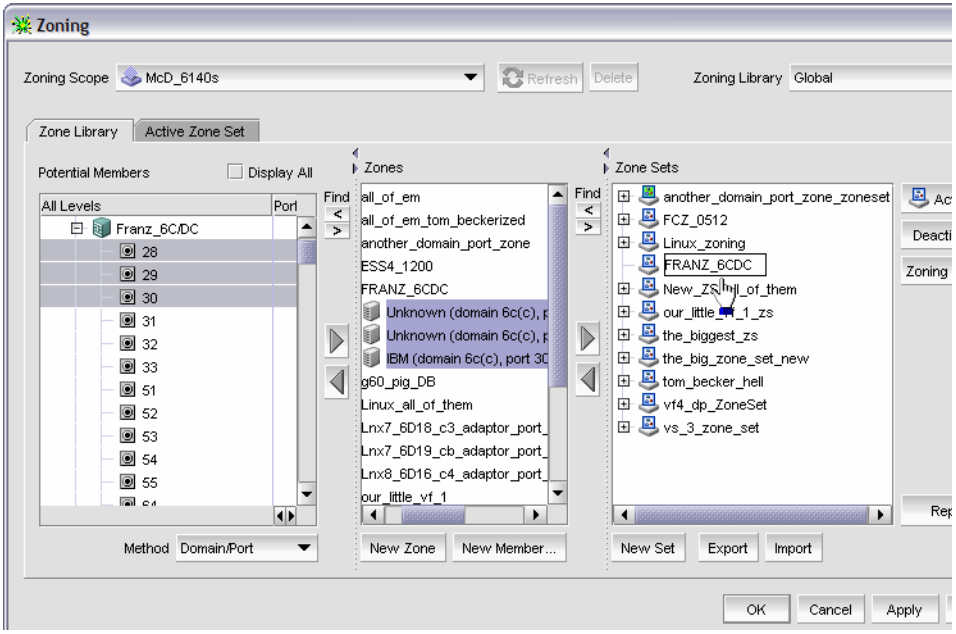

Zoning
Zoning Scope
McD_6140s
Refresh
Delete
Zoning Library
Global
Zone Library
Active Zone Set
Potential Members
☐ Display All
All Levels
Port
Franz_6C/DC
28
29
30
31
32
33
51
52
53
54
55
Find
<
>
Zones
all_of_em
all_of_em_tom_beckerized
another_domain_port_zone
ESS4_1200
FRANZ_6CDC
Unknown (domain 6c(c), p
Unknown (domain 6c(c), p
IBM (domain 6c(c), port 30
g60_pig_DB
Linux_all_of_them
Lnx7_6D18_c3_adaptor_port_
Lnx7_6D19_cb_adaptor_port_
Lnx8_6D16_c4_adaptor_port_
our_little_vf_1
Zone Sets
another_domain_port_zone_zoneset
FCZ_0512
Linux_zoning
New_ZS_all_of_them
our_little_vf_1_zs
the_biggest_zs
the_big_zone_set_new
tom_becker_hell
vf4_dp_ZoneSet
vs_3_zone_set
Ac
Deacti
Zoning
Rep
Method
Domain/Port
New Zone
New Member...
New Set
Export
Import
OK
Cancel
Apply

Figure 2-266 Create new zone set

We create a new zone set as shown in Figure 2-267 and Figure 2-268.

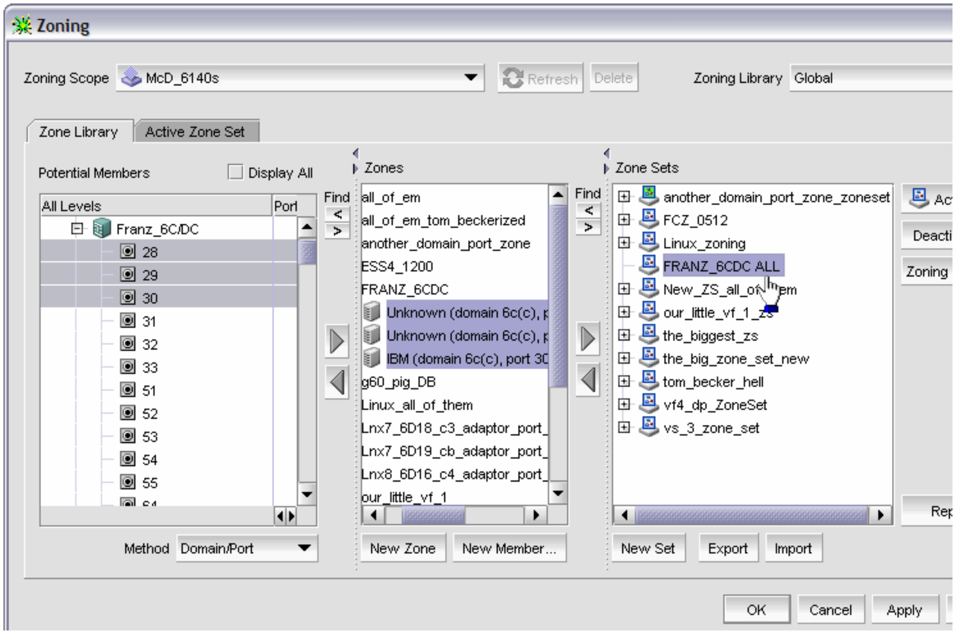

Zoning
Refresh
Delete
Zone Library
Active Zone Set
Potential Members
☐ Display All
All Levels
Port
Franz_6C/DC
28
29
30
31
32
33
51
52
53
54
55
Find
Zones
all_of_em
all_of_em_tom_beckerized
another_domain_port_zone
ESS4_1200
FRANZ_6CDC
Unknown (domain 6c(c), p
Unknown (domain 6c(c), p
IBM (domain 6c(c), port 30
g60_pig_DB
Linux_all_of_them
Lnx7_6D18_c3_adaptor_port_
Lnx7_6D19_cb_adaptor_port_
Lnx8_6D16_c4_adaptor_port_
our_little_vf_1
Zone Sets
another_domain_port_zone_zoneset
FCZ_0512
Linux_zoning
FRANZ_6CDC
New_ZS_all_of_them
our_little_vf_1_zs
the_biggest_zs
the_big_zone_set_new
tom_becker_hell
vf4_dp_ZoneSet
vs_3_zone_set
Ac
Deacti
Zoning
Rep
New Zone
New Member...
New Set
Export
Import
OK
Cancel
Apply

Zoning Scope: McD_6140s

Zoning Library: Global

Method: Domain/Port

Figure 2-267 Create new zone set - 1/2


Zoning
Refresh
Delete
Zone Library
Active Zone Set
Potential Members
☐ Display All
All Levels
Port
Franz_6C/DC
28
29
30
31
32
33
51
52
53
54
55
Find
Zones
all_of_em
all_of_em_tom_beckerized
another_domain_port_zone
ESS4_1200
FRANZ_6CDC
Unknown (domain 6c(c), p
Unknown (domain 6c(c), p
IBM (domain 6c(c), port 30
g60_pig_DB
Linux_all_of_them
Lnx7_6D18_c3_adaptor_port_
Lnx7_6D19_cb_adaptor_port_
Lnx8_6D16_c4_adaptor_port_
our_little_vf_1
Zone Sets
another_domain_port_zone_zoneset
FCZ_0512
Linux_zoning
FRANZ_6CDC ALL
New_ZS_all_of_them
our_little_vf_1_zs
the_biggest_zs
the_big_zone_set_new
tom_becker_hell
vf4_dp_ZoneSet
vs_3_zone_set
Ac
Deacti
Zoning
Rep
New Zone
New Member...
New Set
Export
Import
OK
Cancel
Apply

Zoning Scope: McD_6140s

Zoning Library: Global

Method: Domain/Port

Figure 2-268 Create new zone set - 2/2

We display the options available to us by right-clicking the zone set name as shown in Figure 2-269.

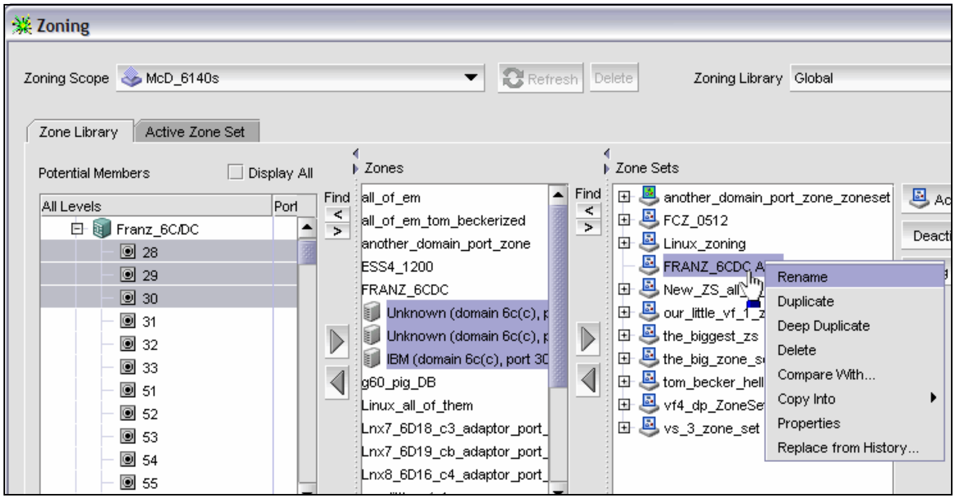

Zoning
Zoning Scope
McD_6140s
Refresh
Delete
Zoning Library
Global
Zone Library
Active Zone Set
Potential Members
Display All
All Levels
Port
Franz_6C/DC
28
29
30
31
32
33
51
52
53
54
55
Find
Zones
all_of_em
all_of_em_tom_beckerized
another_domain_port_zone
ESS4_1200
FRANZ_6CDC
Unknown (domain 6c(c), p
Unknown (domain 6c(c), p
IBM (domain 6c(c), port 30
g60_pig_DB
Linux_all_of_them
Lnx7_6D18_c3_adaptor_port_
Lnx7_6D19_cb_adaptor_port_
Lnx8_6D16_c4_adaptor_port_
Zone Sets
another_domain_port_zone_zoneset
FCZ_0512
Linux_zoning
FRANZ_6CDC A
New_ZS_all
our_little_vf_1_z
the_biggest_zs
the_big_zone_s
tom_becker_hell
vf4_dp_ZoneSe
vs_3_zone_set
Rename
Duplicate
Deep Duplicate
Delete
Compare With...
Copy Into
Properties
Replace from History...
Ac
Deacti

Figure 2-269 Displaying options

We now place our new zone in the new zone set as shown in Figure 2-270 and Figure 2-271.

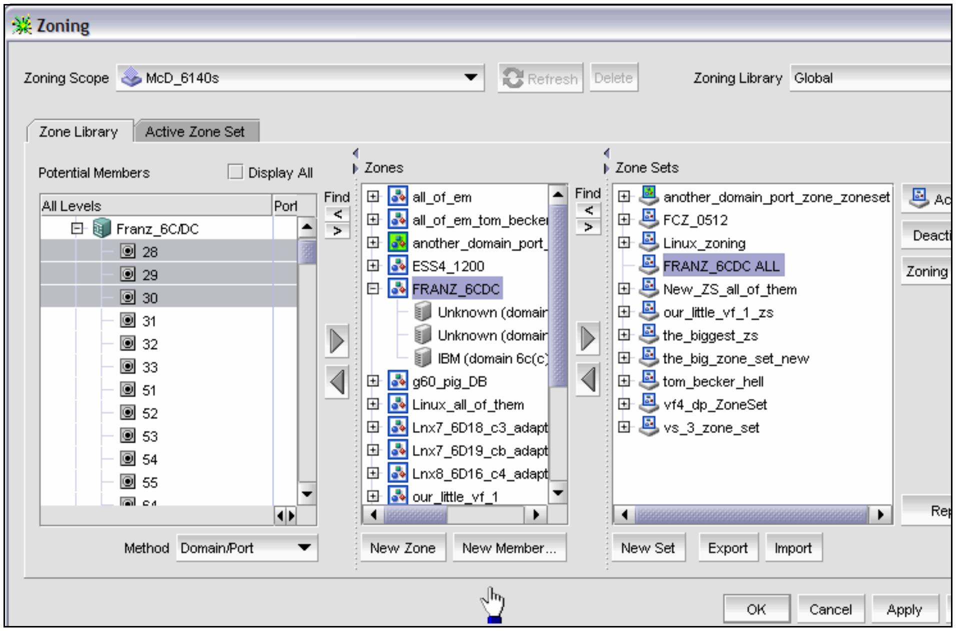

Zoning
Zoning Scope
McD_6140s
Refresh
Delete
Zoning Library
Global
Zone Library
Active Zone Set
Potential Members
Display All
All Levels
Port
Franz_6C/DC
28
29
30
31
32
33
51
52
53
54
55
Find
Zones
all_of_em
all_of_em_tom_becke
another_domain_port_
ESS4_1200
FRANZ_6CDC
Unknown (domain
Unknown (domain
IBM (domain 6c(c)
g60_pig_DB
Linux_all_of_them
Lnx7_6D18_c3_adapt
Lnx7_6D19_cb_adapt
Lnx8_6D16_c4_adapt
our_little_vf_1
Zone Sets
another_domain_port_zone_zoneset
FCZ_0512
Linux_zoning
FRANZ_6CDC ALL
New_ZS_all_of_them
our_little_vf_1_zs
the_biggest_zs
the_big_zone_set_new
tom_becker_hell
vf4_dp_ZoneSet
vs_3_zone_set
Ac
Deacti
Zoning
Rep
Method
Domain/Port
New Zone
New Member...
New Set
Export
Import
OK
Cancel
Apply

Figure 2-270 Zone into zone set - 1/2

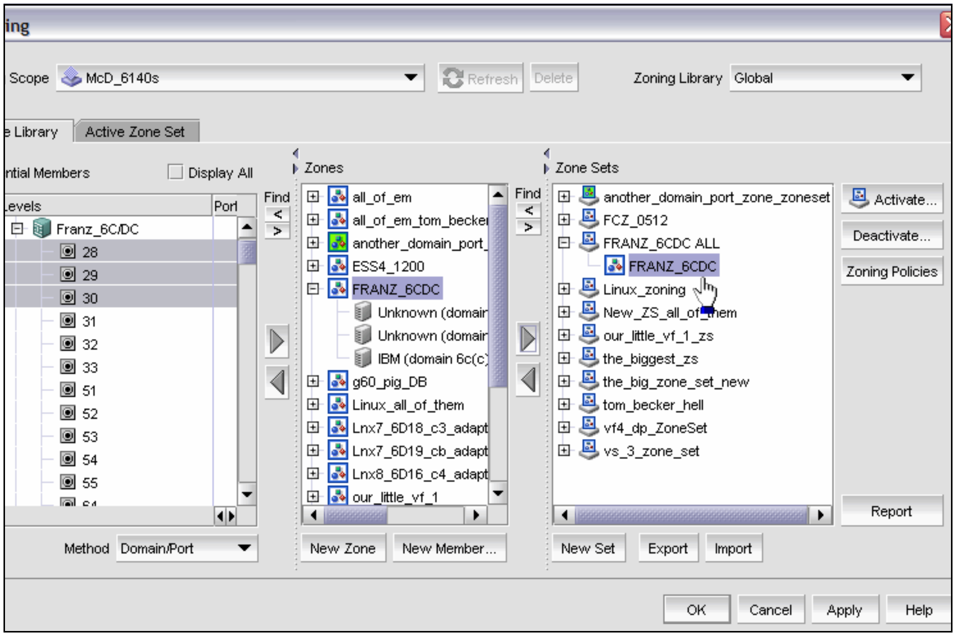

ing
Scope
McD_6140s
Refresh
Delete
Zoning Library
Global
e Library
Active Zone Set
ntial Members
Display All
Levels
Port
Franz_6C/DC
28
29
30
31
32
33
51
52
53
54
55
Find
Zones
all_of_em
all_of_em_tom_becker
another_domain_port_
ESS4_1200
FRANZ_6CDC
Unknown (domain
Unknown (domain
IBM (domain 6c(c)
g60_pig_DB
Linux_all_of_them
Lnx7_6D18_c3_adapt
Lnx7_6D19_cb_adapt
Lnx8_6D16_c4_adapt
our_little_vf_1
Zone Sets
another_domain_port_zone_zoneset
FCZ_0512
FRANZ_6CDC ALL
FRANZ_6CDC
Linux_zoning
New_ZS_all_of_them
our_little_vf_1_zs
the_biggest_zs
the_big_zone_set_new
tom_becker_hell
vf4_dp_ZoneSet
vs_3_zone_set
Activate...
Deactivate...
Zoning Policies
Report
Method
Domain/Port
New Zone
New Member...
New Set
Export
Import
OK
Cancel
Apply
Help

Figure 2-271 Zone into zone set - 2/2

To activate the zone set, click the **Activate** button.

2.26.8 Activating FICON CUP Zoning

When the FCZ feature key has been added to the system, enable it to make it active. Open the Element Manager, select **Configure** →**FICON Management Server** →**Enable FMS**, as shown in Figure 2-272.

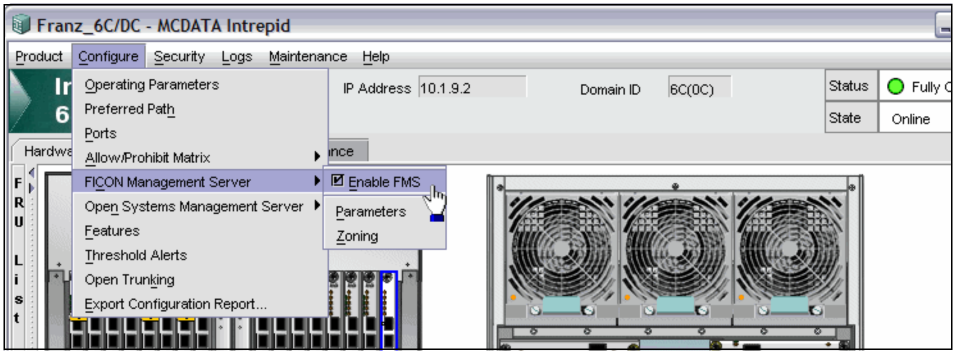
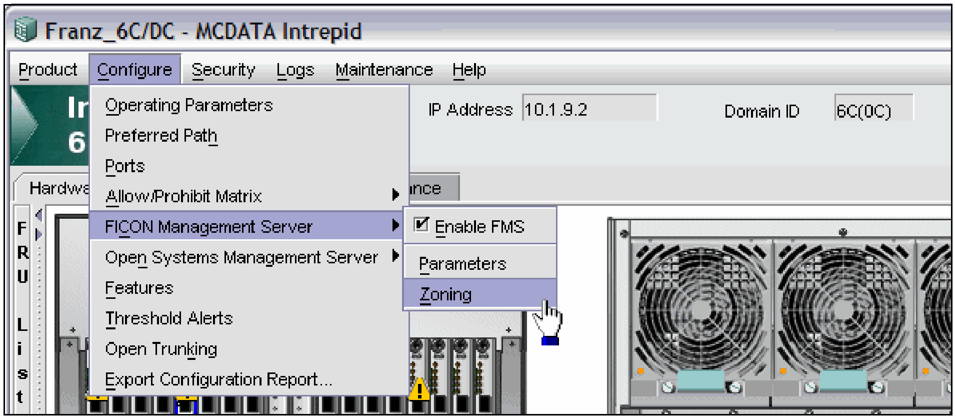

Franz_6C/DC - MCDATA Intrepid
Product
Configure
Security
Logs
Maintenance
Help
Operating Parameters
Preferred Path
Ports
Allow/Prohibit Matrix
FICON Management Server
Open Systems Management Server
Features
Threshold Alerts
Open Trunking
Export Configuration Report...
Enable FMS
Parameters
Zoning
IP Address
10.1.9.2
Domain ID
6C(0C)
Status
Fully
State
Online
Hardwa
FRU List

Figure 2-272 FICON management server

Click **Zoning** as shown in Figure 2-273.


Franz_6C/DC - MCDATA Intrepid
Product
Configure
Security
Logs
Maintenance
Help
Operating Parameters
Preferred Path
Ports
Allow/Prohibit Matrix
FICON Management Server
Open Systems Management Server
Features
Threshold Alerts
Open Trunking
Export Configuration Report...
Enable FMS
Parameters
Zoning
Hardwa
nce
FRU List

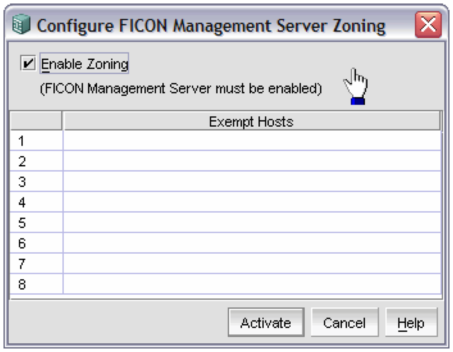
IP Address 10.1.9.2

Domain ID 6C(0C)

☑ Enable FMS

Figure 2-273 Configure zoning

The Configure FICON Management Server Zoning dialog box displays as shown in Figure 2-274, and put a check mark in the **Enable Zoning** box, and click **Activate**.


Configure FICON Management Server Zoning
Exempt Hosts
1
2
3
4
5
6
7
8
Activate
Cancel
Help

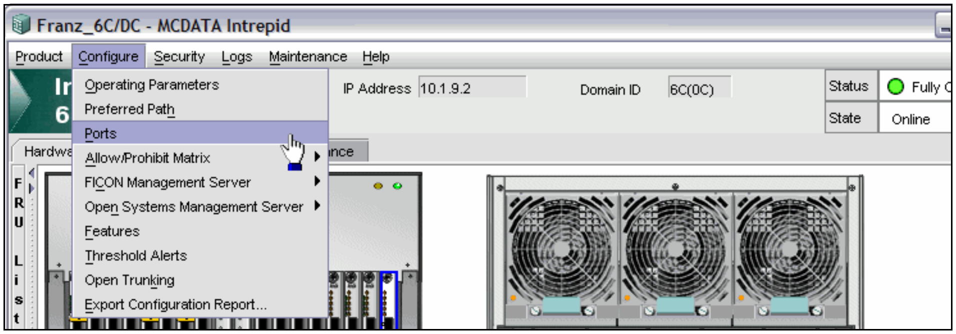
☑ Enable Zoning
(FICON Management Server must be enabled)

Figure 2-274 Enable zoning

FCZ is now installed and activated.

2.26.9 Configuring ISL credits and port speed

Although an optional step, in most cascaded environments, extended buffer-to-buffer (BB) credits are set. To set buffer credits from Element Manager, we select **Configure** →**Ports** as shown in Figure 2-275.


Franz_6C/DC - MCDATA Intrepid
Product
Configure
Security
Logs
Maintenance
Help
Operating Parameters
Preferred Path
Ports
Allow/Prohibit Matrix
FICON Management Server
Open Systems Management Server
Features
Threshold Alerts
Open Trunking
Export Configuration Report...
Hardwa
nce
FRU List

IP Address 10.1.9.2

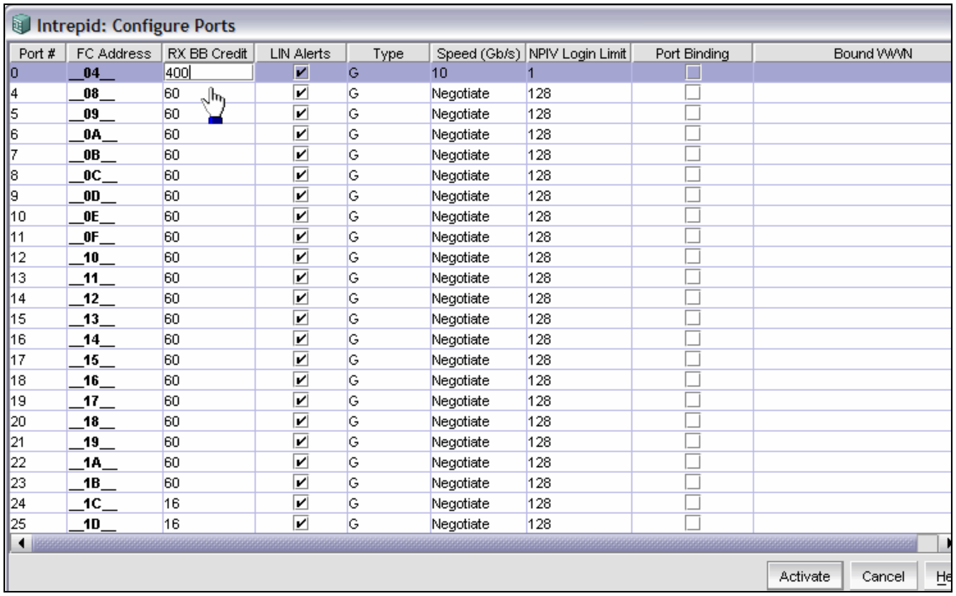
Domain ID 6C(0C)

Status Fully C

State Online

Figure 2-275 Configure ports

The pop-up menu displays as in shown in Figure 2-276.


Intrepid: Configure Ports
Activate
Cancel
He

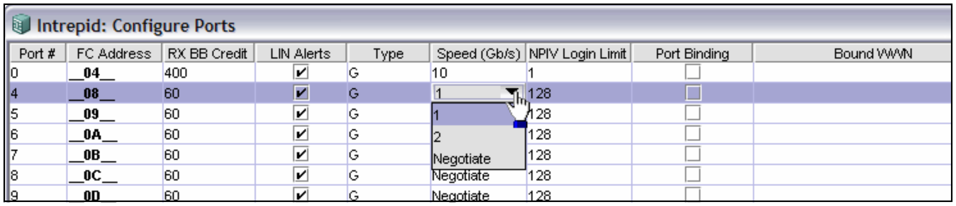
Port #	FC Address	RX BB Credit	LIN Alerts	Type	Speed (Gb/s)	NPIV Login Limit	Port Binding	Bound WWN
0	__04__	400	☑	G	10	1	☐	
4	__08__	60	☑	G	Negotiate	128	☐	
5	__09__	60	☑	G	Negotiate	128	☐	
6	__0A__	60	☑	G	Negotiate	128	☐	
7	__0B__	60	☑	G	Negotiate	128	☐	
8	__0C__	60	☑	G	Negotiate	128	☐	
9	__0D__	60	☑	G	Negotiate	128	☐	
10	__0E__	60	☑	G	Negotiate	128	☐	
11	__0F__	60	☑	G	Negotiate	128	☐	
12	__10__	60	☑	G	Negotiate	128	☐	
13	__11__	60	☑	G	Negotiate	128	☐	
14	__12__	60	☑	G	Negotiate	128	☐	
15	__13__	60	☑	G	Negotiate	128	☐	
16	__14__	60	☑	G	Negotiate	128	☐	
17	__15__	60	☑	G	Negotiate	128	☐	
18	__16__	60	☑	G	Negotiate	128	☐	
19	__17__	60	☑	G	Negotiate	128	☐	
20	__18__	60	☑	G	Negotiate	128	☐	
21	__19__	60	☑	G	Negotiate	128	☐	
22	__1A__	60	☑	G	Negotiate	128	☐	
23	__1B__	60	☑	G	Negotiate	128	☐	
24	__1C__	16	☑	G	Negotiate	128	☐	
25	__1D__	16	☑	G	Negotiate	128	☐	

Figure 2-276 Change BB credits

Enter the number of buffer credits in the “RX BB Credit” column. For the 6064 and 6140, this should be 60 for ISL ports. For the i10K, you have to calculate the required BB credits. We have selected 400.

To set the port speed for all ports, move the cursor to the *Speed* column and right-click for a drop-down menu of available port speeds, as shown in Figure 2-277.

To change the speed of an individual port, left-click for a pull-down menu of available speeds. The recommended best practice is to leave the speed setting at *Negotiate* and only change the speed setting if a port does not log in properly. Typically, auto-negotiate is only a problem with 1 Gbps DWDM equipment and occasionally an older 1 Gbps control unit interface.

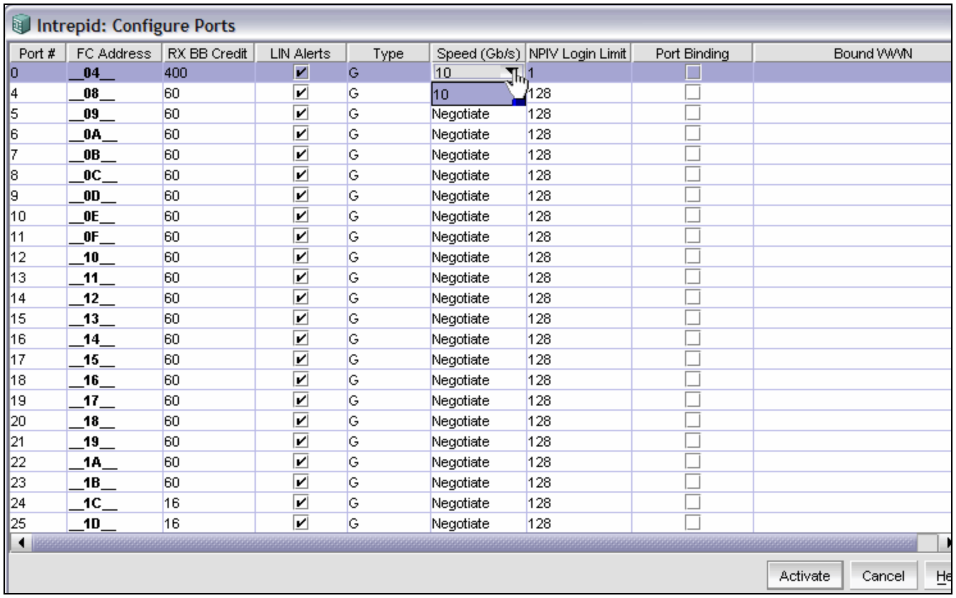


Intrepid: Configure Ports

Port #	FC Address	RX BB Credit	LIN Alerts	Type	Speed (Gb/s)	NPIV Login Limit	Port Binding	Bound WWN
0	__04__	400	☑	G	10	1	☐	
4	__08__	60	☑	G	1	128	☐	
5	__09__	60	☑	G	1	128	☐	
6	__0A__	60	☑	G	2	128	☐	
7	__0B__	60	☑	G	Negotiate	128	☐	
8	__0C__	60	☑	G	Negotiate	128	☐	
9	__0D__	60	☑	G	Negotiate	128	☐	

Figure 2-277 Changing port speed

We have a 10 Gbps ISL available, so we have set it to 10 as shown in Figure 2-278.



Intrepid: Configure Ports

Port #	FC Address	RX BB Credit	LIN Alerts	Type	Speed (Gb/s)	NPIV Login Limit	Port Binding	Bound WWN
0	__04__	400	☑	G	10	1	☐	
4	__08__	60	☑	G	10	128	☐	
5	__09__	60	☑	G	Negotiate	128	☐	
6	__0A__	60	☑	G	Negotiate	128	☐	
7	__0B__	60	☑	G	Negotiate	128	☐	
8	__0C__	60	☑	G	Negotiate	128	☐	
9	__0D__	60	☑	G	Negotiate	128	☐	
10	__0E__	60	☑	G	Negotiate	128	☐	
11	__0F__	60	☑	G	Negotiate	128	☐	
12	__10__	60	☑	G	Negotiate	128	☐	
13	__11__	60	☑	G	Negotiate	128	☐	
14	__12__	60	☑	G	Negotiate	128	☐	
15	__13__	60	☑	G	Negotiate	128	☐	
16	__14__	60	☑	G	Negotiate	128	☐	
17	__15__	60	☑	G	Negotiate	128	☐	
18	__16__	60	☑	G	Negotiate	128	☐	
19	__17__	60	☑	G	Negotiate	128	☐	
20	__18__	60	☑	G	Negotiate	128	☐	
21	__19__	60	☑	G	Negotiate	128	☐	
22	__1A__	60	☑	G	Negotiate	128	☐	
23	__1B__	60	☑	G	Negotiate	128	☐	
24	__1C__	16	☑	G	Negotiate	128	☐	
25	__1D__	16	☑	G	Negotiate	128	☐	

Figure 2-278 ISL speed

When done, select **Activate**.

2.26.10 Enabling FICON Management Server (CUP)

Although CUP is not a required feature, it is often included. Simply loading the feature key does not actually enable it. Enable CUP on each director by selecting **Enable FMS** as shown in Figure 2-279.

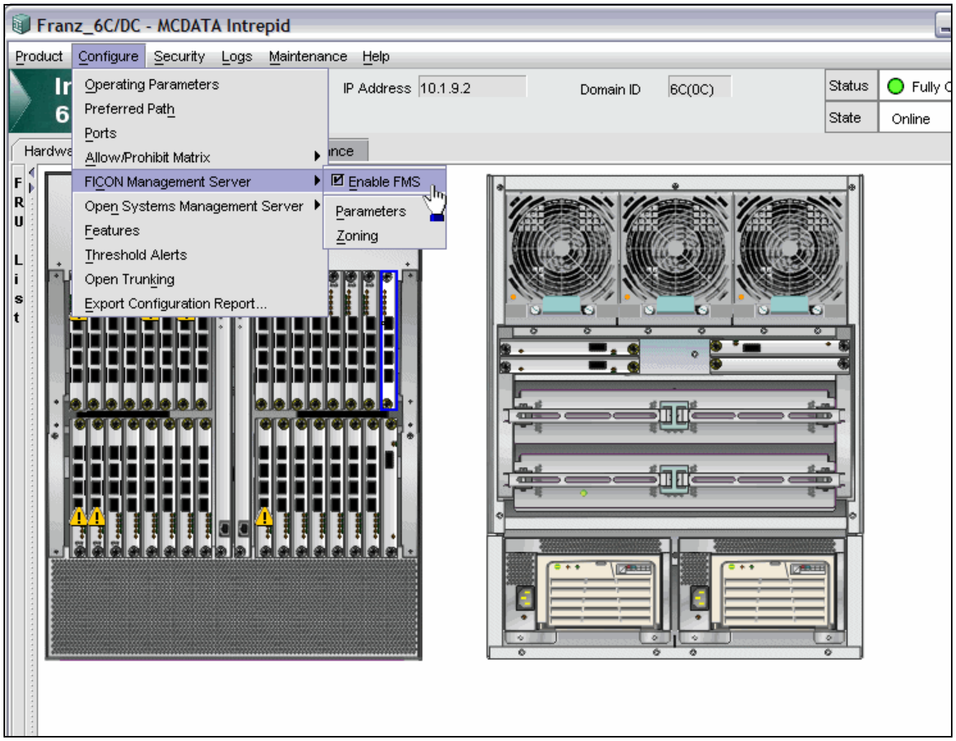
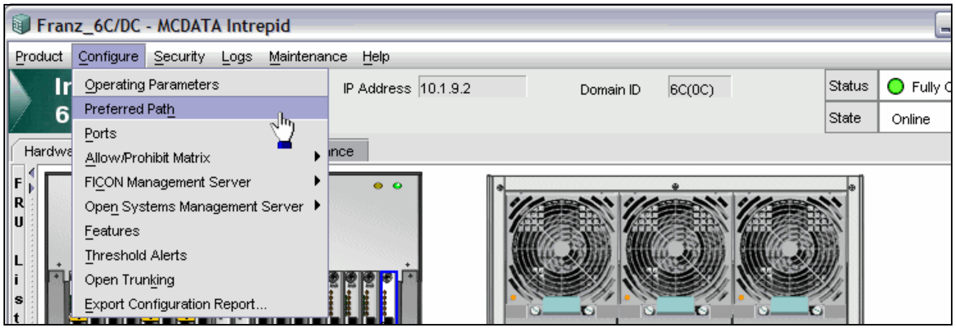

Franz_6C/DC - MCDATA Intrepid
Product
Configure
Security
Logs
Maintenance
Help
Operating Parameters
Preferred Path
Ports
Allow/Prohibit Matrix
FICON Management Server
Open Systems Management Server
Features
Threshold Alerts
Open Trunking
Export Configuration Report...
☑ Enable FMS
Parameters
Zoning
IP Address
10.1.9.2
Domain ID
6C(0C)
Status
Fully O
State
Online
Hardwa
FRU List

Figure 2-279 Enabling FMS

2.26.11 Setting preferred paths

Select the **Preferred Path** option from the Element Manager application's Configure menu as shown in Figure 2-280.


Franz_6C/DC - MCDATA Intrepid
Product
Configure
Security
Logs
Maintenance
Help
Operating Parameters
Preferred Path
Ports
Allow/Prohibit Matrix
FICON Management Server
Open Systems Management Server
Features
Threshold Alerts
Open Trunking
Export Configuration Report...
Hardwa
nce
F R U L i s t

IP Address 10.1.9.2

Domain ID 6C(0C)

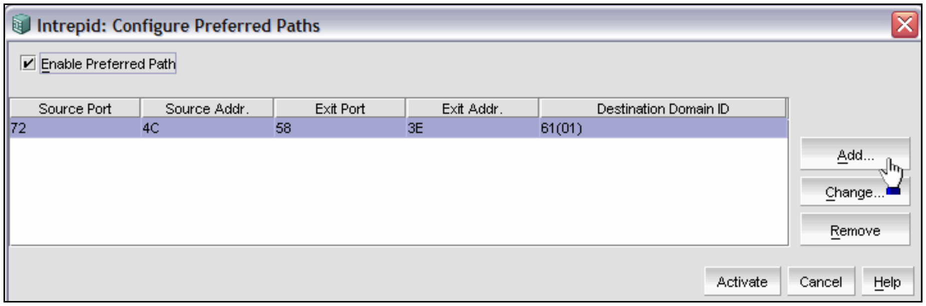
Status Fully C

State Online

Figure 2-280 Configuring preferred paths

The Configure Preferred Paths dialog box displays. The process shown in the window captures from Figure 2-281 through to Figure 2-285 is as follows:

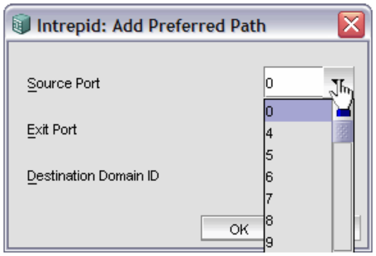
1. Click **Add**. The Add Preferred Path dialog box displays.
2. For the director entry port, type logical port number of the channel or control unit port in the Source Port field. For the director exit port, type the logical port number of the ISL in the Exit Port field. For the destination device, put the domain ID (not the switch address) in the Destination Domain ID field.
3. Click **OK** to save the path configuration and close the dialog box.


Intrepid: Configure Preferred Paths
Add...
Change...
Remove
Activate
Cancel
Help

☑ Enable Preferred Path

Source Port	Source Addr.	Exit Port	Exit Addr.	Destination Domain ID
72	4C	58	3E	61(01)

Figure 2-281 Adding preferred path

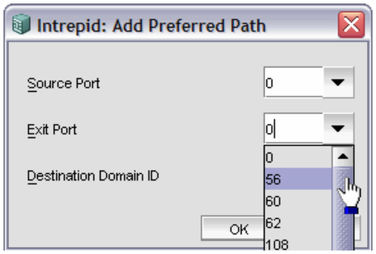

Intrepid: Add Preferred Path
0
4
5
6
7
8
9
OK

Source Port 0

Exit Port

Destination Domain ID

Figure 2-282 Choosing source port

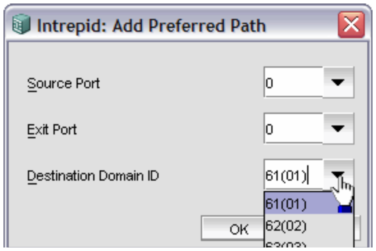

Intrepid: Add Preferred Path
0
56
60
62
108
OK

Source Port 0

Exit Port 0

Destination Domain ID

Figure 2-283 Choosing exit port

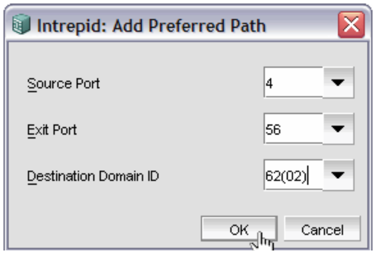

Intrepid: Add Preferred Path
61(01)
62(02)
OK

Source Port 0

Exit Port 0

Destination Domain ID 61(01)

Figure 2-284 Choosing destination Domain ID


Intrepid: Add Preferred Path
OK
Cancel

Source Port 4

Exit Port 56

Destination Domain ID 62(02)

Figure 2-285 Selecting OK

This procedure must be repeated for each director and each port for which the preferred path is being defined.

2.26.12 Set Open Trunking

Open Trunking is only available if the optional Open Trunking feature is installed. Select **Configure** →**Configure Open Trunking**. The Configure Open Trunking dialog box displays as shown in Figure 2-286.

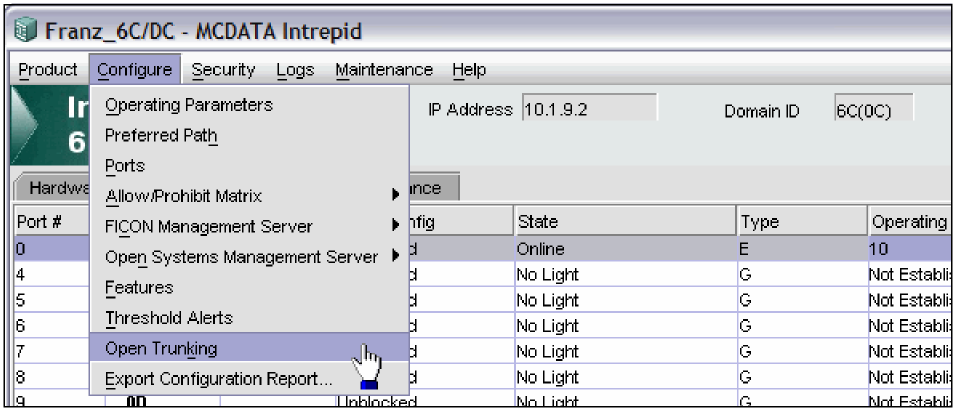
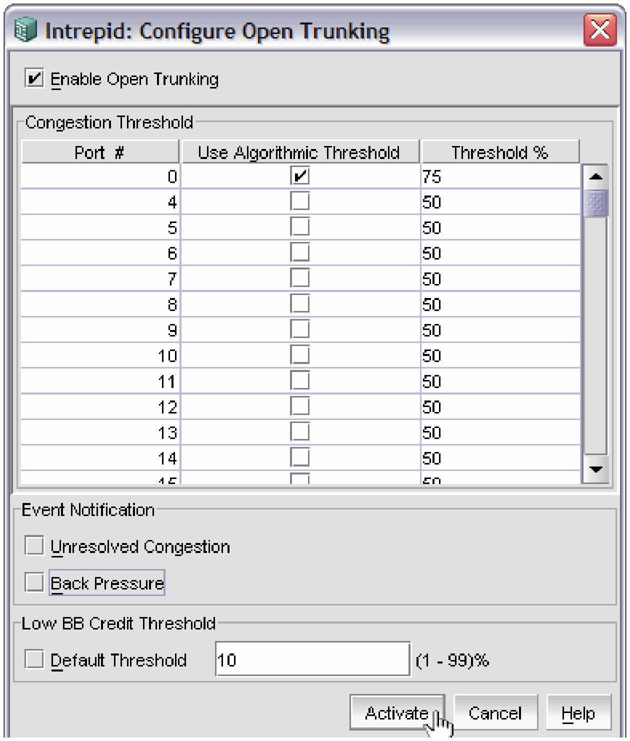

Franz_6C/DC - MCDATA Intrepid
Product
Configure
Security
Logs
Maintenance
Help
Operating Parameters
Preferred Path
Ports
Allow/Prohibit Matrix
FICON Management Server
Open Systems Management Server
Features
Threshold Alerts
Open Trunking
Export Configuration Report...
IP Address
10.1.9.2
Domain ID
6C(0C)
Port #
State
Type
Operating

Figure 2-286 Configure Open Trunking

The pop-up menu shown in Figure 2-287 displays.



☑ Enable Open Trunking

Congestion Threshold

Port #	Use Algorithmic Threshold	Threshold %
0	☑	75
4	☐	50
5	☐	50
6	☐	50
7	☐	50
8	☐	50
9	☐	50
10	☐	50
11	☐	50
12	☐	50
13	☐	50
14	☐	50

Event Notification

☐ Unresolved Congestion

☐ Back Pressure

Low BB Credit Threshold

☐ Default Threshold 10 (1 - 99)%

Figure 2-287 Configure Open trunking pop-up menu

Check the **Enable Open** trunking box to enable Open Trunking.

Checking the **Unresolved Congestion** box causes an alert message to be generated anytime congestion on a link is encountered that cannot be moved to another link. Since connections cannot be changed “mid-flight,” this situation can occur after multiple connections are established, but the nature of traffic is such that connections on one ISL are more heavily utilized than others.

A Back Pressure event occurs when the percentage of time the ISL has no available BB_Credit exceeds the Low BB Credit threshold. A separate event also occurs when the back pressure condition ends.

Low BB Credit Threshold is the percentage of time that the transmitting link has no BB_Credit. This value is also used when determining routes for a transmit link. An ISL that has no BB_Credit for longer than this time percentage cannot be the recipient of traffic rerouted from other ISLs. Traffic on this ISL might be rerouted by Open Trunking, even if the ISL is not congested.

2.26.13 Configuring the Allow/Prohibit matrix

The allow/prohibit operations are configured using the configure addresses dialog. They affect port-to-port connectivity and are applied *in addition* to the zoning information. Therefore, configure the allow/prohibit permissions in EFCM to reflect the zoning configuration. Each member of a common zone should be configured to *allow* access to all other members of the zone, and members from different zones should be configured with *prohibited* access to members in other zones.

An *X* in the matrix prohibits certain connections. This can be used to enforce security precautions. It can also be useful in cascaded environments with certain network devices that pipeline data to restrict data flow to certain ISLs.

> **Note:** Always Prohibit ISL Ports: A multi-hop cascaded FICON is not supported so there is never a requirement for one ISL port (E_Port) to talk to another ISL port. Prohibiting ISLs ports from communicating with one another guarantees that an unsupported path is not inadvertently taken.

When the *Active=Saved* attribute is set, the active PDCM is saved so that in the event of total power failure, or when recovering an EFCM, the last active PDCM matrix is restored. Typically, the *Active=Saved* attribute should be set.

From the Element Manager, select **Active** as shown in Figure 2-288.

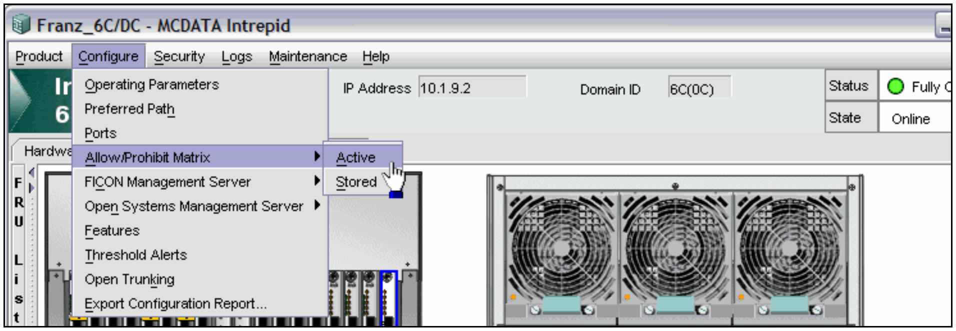
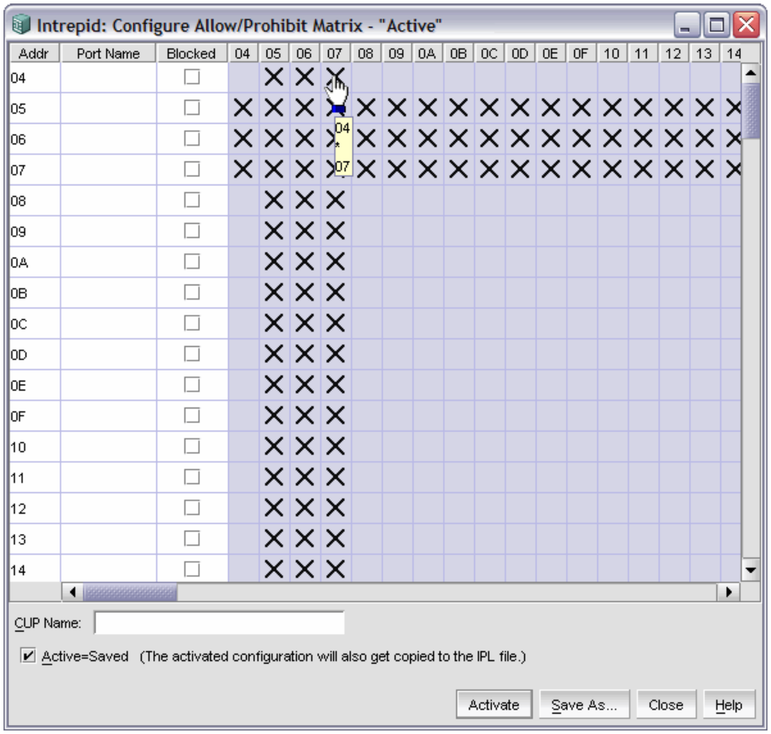

Franz_6C/DC - MCDATA Intrepid
Product
Configure
Security
Logs
Maintenance
Help
Operating Parameters
Preferred Path
Ports
Allow/Prohibit Matrix
FICON Management Server
Open Systems Management Server
Features
Threshold Alerts
Open Trunking
Export Configuration Report...
Active
Stored
IP Address
10.1.9.2
Domain ID
6C(0C)
Status
Fully C
State
Online
Hardwa
FRU List

Figure 2-288 Active

The pop-up menu displays as shown in Figure 2-289.



Addr	Port Name	Blocked	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14
04		☐		X	X	X													
05		☐	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
06		☐	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
07		☐	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
08		☐		X	X	X													
09		☐		X	X	X													
0A		☐		X	X	X													
0B		☐		X	X	X													
0C		☐		X	X	X													
0D		☐		X	X	X													
0E		☐		X	X	X													
0F		☐		X	X	X													
10		☐		X	X	X													
11		☐		X	X	X													
12		☐		X	X	X													
13		☐		X	X	X													
14		☐		X	X	X													

CUP Name:

☑ Active=Saved (The activated configuration will also get copied to the IPL file.)

Figure 2-289 Matrix

Place the cursor in the matrix and left click to change the state. An "X" indicates that communication between these two ports is prohibited. Even if you do not intend to prohibit any connections, you should at least set *Active=Saved*.

2.26.14 Enabling binding features

Binding is necessary for two-byte addressing. The only time binding should be set in a non-cascaded environment is when binding is being used for security purposes (which is very rare for mainframe environments). Only Fabric Binding is required for two-byte addressing, but you can choose other binding methods. Fabric Binding is the most common method of binding for FICON.

It is much easier to set up the binding features after all connections are made so that all WWNs that have to be added to binding tables have been discovered.

When enabled, changing the method of binding is an offline function.

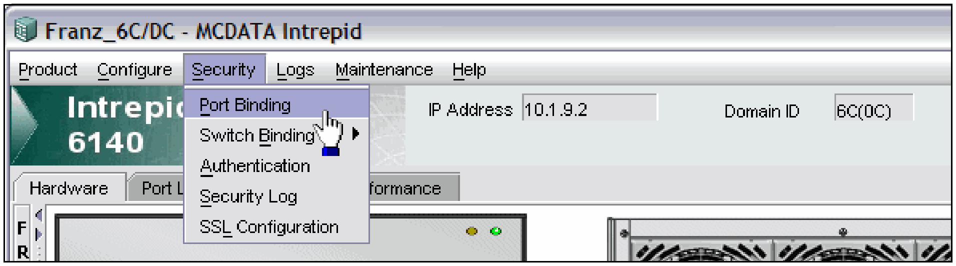
> **Attention:** Anytime a channel with two-byte addressing defined is connected to a fabric, every switch in that fabric must meet the minimum requirements for two-byte addressing.

2.26.15 Enabling port binding

Port binding is very rarely, if ever, used in mainframe environments. Make sure that the client clearly understands what port binding is before proceeding.

> **Important:** The switch rejects any connection if the node for that connection is not in the port binding membership list. Mainframes turn off light on channels when the connection is rejected so the WWN will not be available in EFCM to add to the membership list.

Port binding is typically done from the element manager as in Figure 2-290.

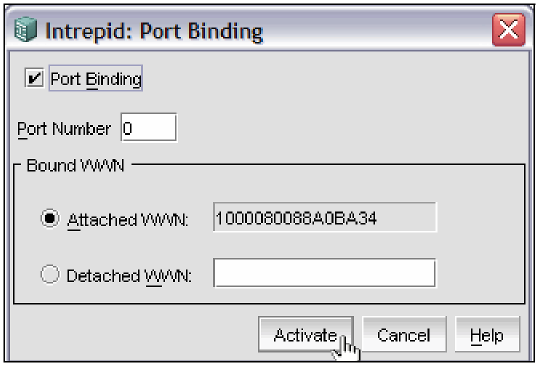

Franz_6C/DC - MCDATA Intrepid
Product
Configure
Security
Logs
Maintenance
Help
Port Binding
Switch Binding
Authentication
Security Log
SSL Configuration
Intrepid
6140
Hardware
Port L
formance

IP Address 10.1.9.2

Domain ID 6C(0C)

Figure 2-290 Port binding

The menu in Figure 2-291 displays.


Intrepid: Port Binding
Bound WWN
Activate
Cancel
Help

☑ Port Binding

Port Number 0

● Attached WWN: 1000080088A0BA34

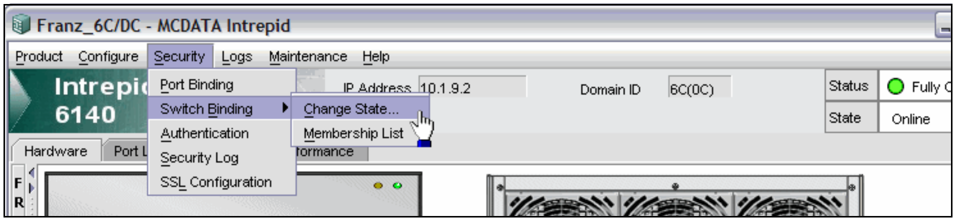
○ Detached WWN:

Figure 2-291 Enabling Port Binding

By checking the Port Binding box, and selecting **Attached WWN**, the WWNs of all attached HBAs and devices are put in the Port Binding membership list. Selecting **Detached WWN** allows you to define a switch and its ports that are not in the fabric yet. It is much easier to make all the desired attachments first so that all WWNs are automatically discovered.

2.26.16 Enabling switch binding

To configure switch binding, click **Security** → **Switch Binding** → **Change State** as shown in Figure 2-292.


Franz_6C/DC - MCDATA Intrepid
Product
Configure
Security
Logs
Maintenance
Help
Intrepid
6140
Port Binding
Switch Binding
Authentication
Security Log
SSL Configuration
Change State...
Membership List
Hardware
Port L
formance
F
R

IP Address 10.1.9.2

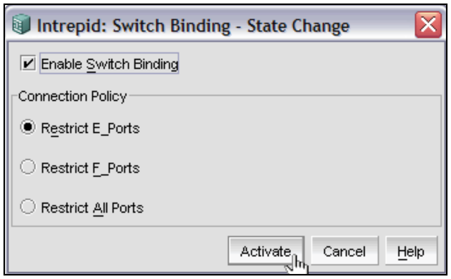
Domain ID 6C(0C)

Status Fully

State Online

Figure 2-292 Switch binding

The pop-up menu shown in Figure 2-293 displays.


Intrepid: Switch Binding - State Change
Connection Policy
Activate
Cancel
Help

☑ Enable Switch Binding

● Restrict E_Ports

○ Restrict F_Ports

○ Restrict All Ports

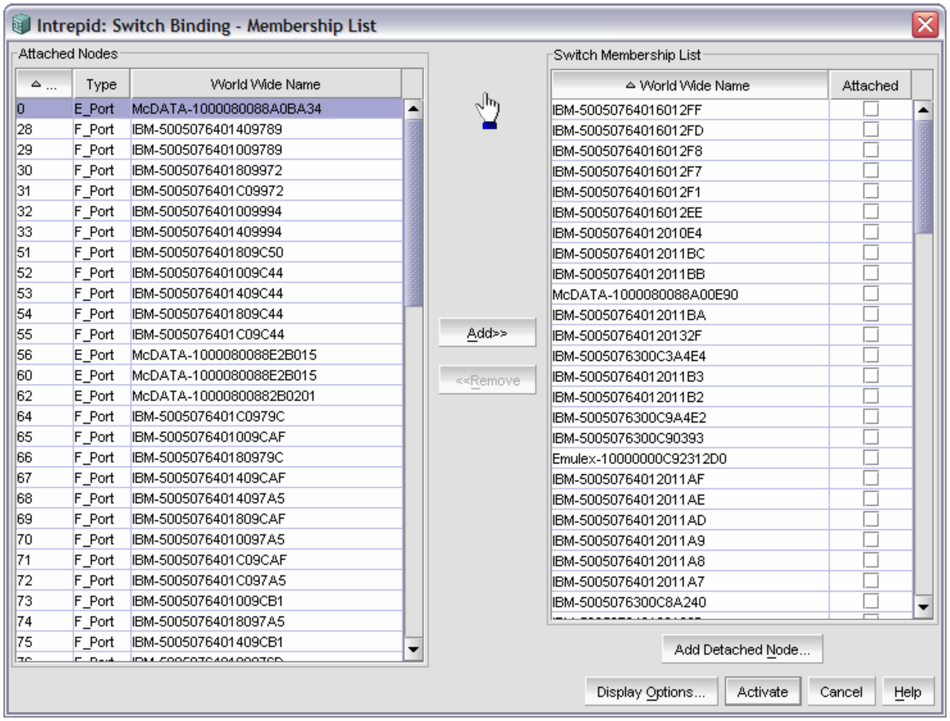
Figure 2-293 Switch binding state change

Click **Enable Switch Binding** to enable switch binding.

Select the type of switch binding (Restrict E_Ports, Restrict F_Ports, or Restrict All Ports). then click **Activate**. In mainframe environments, Restrict E_Ports is the only type of binding that is normally used.

Typically switch binding with Restrict E_Ports is only used in cascaded environments when the data center has limited control over the remote switch. For example, the client is cascading to a switch owned by a disaster recovery service.

Figure 2-294 shows the Attached Nodes and the Switch Membership List.


Intrepid: Switch Binding - Membership List
Attached Nodes
Switch Membership List
Add>>
<<Remove
Add Detached Node...
Display Options...
Activate
Cancel
Help

...	Type	World Wide Name
0	E_Port	McDATA-1000080088A0BA34
28	F_Port	IBM-5005076401409789
29	F_Port	IBM-5005076401009789
30	F_Port	IBM-5005076401809972
31	F_Port	IBM-5005076401C09972
32	F_Port	IBM-5005076401009994
33	F_Port	IBM-5005076401409994
51	F_Port	IBM-5005076401809C50
52	F_Port	IBM-5005076401009C44
53	F_Port	IBM-5005076401409C44
54	F_Port	IBM-5005076401809C44
55	F_Port	IBM-5005076401C09C44
56	E_Port	McDATA-1000080088E2B015
60	E_Port	McDATA-1000080088E2B015
62	E_Port	McDATA-10000800882B0201
64	F_Port	IBM-5005076401C0979C
65	F_Port	IBM-5005076401009CAF
66	F_Port	IBM-500507640180979C
67	F_Port	IBM-5005076401409CAF
68	F_Port	IBM-50050764014097A5
69	F_Port	IBM-5005076401809CAF
70	F_Port	IBM-50050764010097A5
71	F_Port	IBM-5005076401C09CAF
72	F_Port	IBM-5005076401C097A5
73	F_Port	IBM-5005076401009CB1
74	F_Port	IBM-50050764018097A5
75	F_Port	IBM-5005076401409CB1

World Wide Name	Attached
IBM-50050764016012FF	☐
IBM-50050764016012FD	☐
IBM-50050764016012F8	☐
IBM-50050764016012F7	☐
IBM-50050764016012F1	☐
IBM-50050764016012EE	☐
IBM-50050764012010E4	☐
IBM-50050764012011BC	☐
IBM-50050764012011BB	☐
McDATA-1000080088A00E90	☐
IBM-50050764012011BA	☐
IBM-500507640120132F	☐
IBM-5005076300C3A4E4	☐
IBM-50050764012011B3	☐
IBM-50050764012011B2	☐
IBM-5005076300C9A4E2	☐
IBM-5005076300C90393	☐
Emulex-10000000C92312D0	☐
IBM-50050764012011AF	☐
IBM-50050764012011AE	☐
IBM-50050764012011AD	☐
IBM-50050764012011A9	☐
IBM-50050764012011A8	☐
IBM-50050764012011A7	☐
IBM-5005076300C8A240	☐

Figure 2-294 Attached nodes and membership list

2.26.17 Enabling Fabric Binding

To configure Fabric Binding, from View All in EFCM, select **Configure →Fabric Binding** as in Figure 2-295.

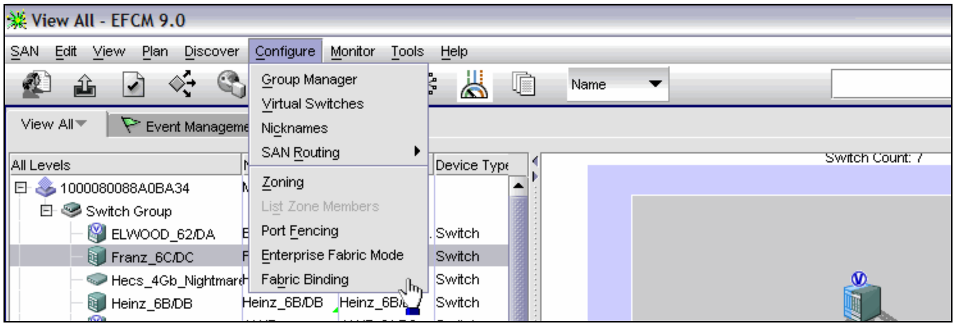
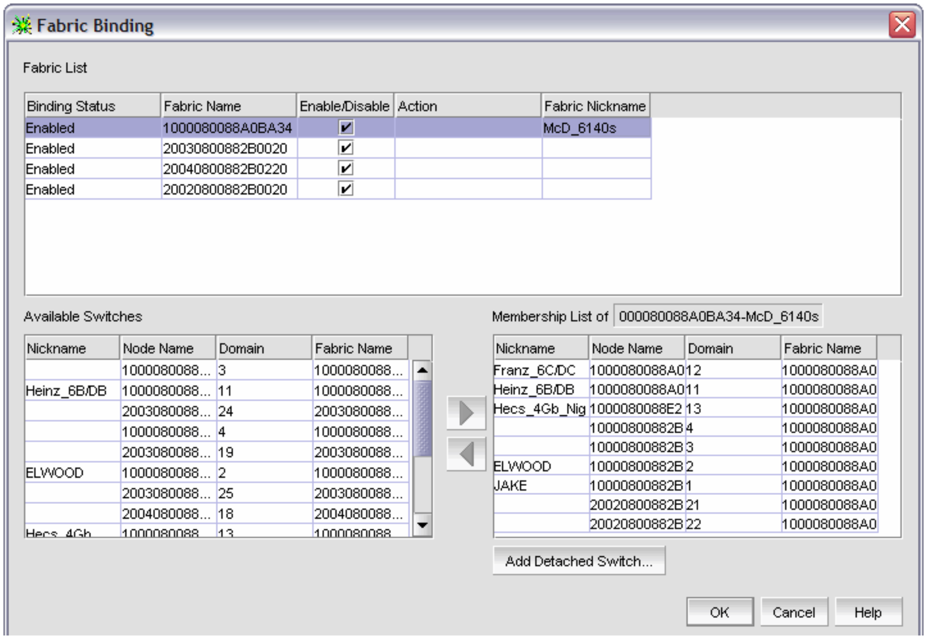

View All - EFCM 9.0
SAN
Edit
View
Plan
Discover
Configure
Monitor
Tools
Help
Group Manager
Virtual Switches
Nicknames
SAN Routing
Zoning
List Zone Members
Port Fencing
Enterprise Fabric Mode
Fabric Binding
Name
View All
Event Manageme
All Levels
Device Type
Switch Count: 7
1000080088A0BA34
Switch Group
ELWOOD_62/DA
Franz_6C/DC
Hecs_4Gb_Nightmare
Heinz_6B/DB
Heinz_6B/DB
Switch
Switch
Switch
Switch

Figure 2-295 Configure Fabric Binding

The window in Figure 2-296 displays.



Fabric List

Binding Status	Fabric Name	Enable/Disable	Action	Fabric Nickname
Enabled	1000080088A0BA34	☑		McD_6140s
Enabled	20030800882B0020	☑		
Enabled	20040800882B0220	☑		
Enabled	20020800882B0020	☑		

Available Switches

Nickname	Node Name	Domain	Fabric Name
	1000080088...	3	1000080088...
Heinz_6B/DB	1000080088...	11	1000080088...
	2003080088...	24	2003080088...
	1000080088...	4	1000080088...
	2003080088...	19	2003080088...
ELWOOD	1000080088...	2	1000080088...
	2003080088...	25	2003080088...
	2004080088...	18	2004080088...
Hecs_4Gb	1000080088	13	1000080088

Membership List of 000080088A0BA34-McD_6140s

Nickname	Node Name	Domain	Fabric Name
Franz_6C/DC	1000080088A0	12	1000080088A0
Heinz_6B/DB	1000080088A0	11	1000080088A0
Hecs_4Gb_Nig	1000080088E2	13	1000080088A0
	10000800882B	4	1000080088A0
	10000800882B	3	1000080088A0
ELWOOD	10000800882B	2	1000080088A0
JAKE	10000800882B	1	1000080088A0
	20020800882B	21	1000080088A0
	20020800882B	22	1000080088A0

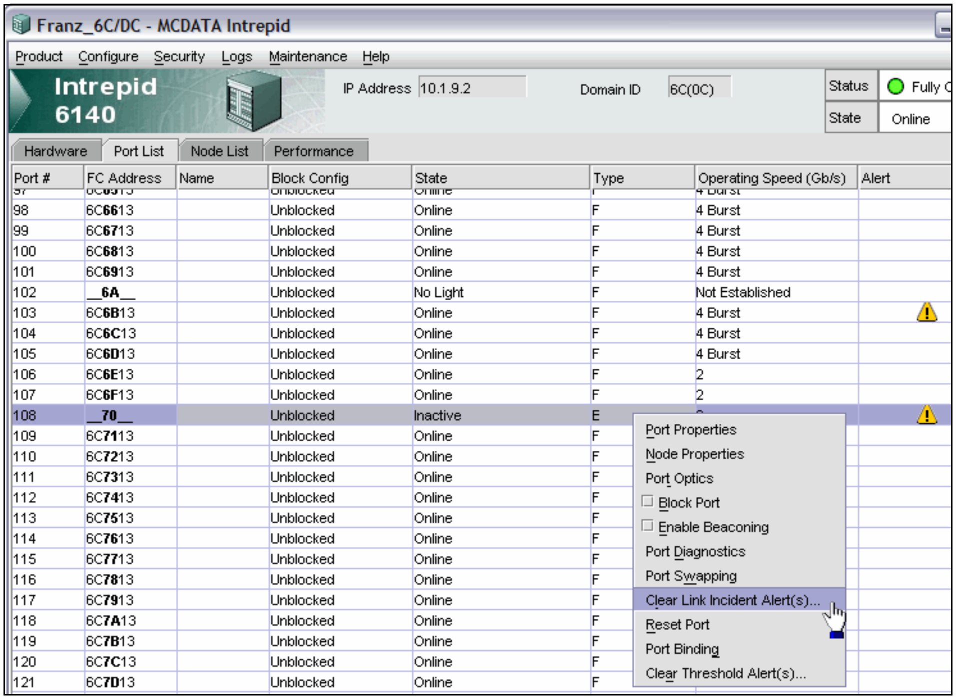
Figure 2-296 Fabric Binding

Enable/Disable in the Fabric List indicates whether Fabric Binding is enabled. Select to enable or disable Fabric Binding for the fabric. Switches interconnected together via an ISL in that fabric appear in the Membership List box in the lower right-hand corner. Click **OK** to enable Fabric Binding on this fabric.

2.26.18 Clearing link alerts

Typically, there are many link incident alerts as a result of normal setup, and the plugging and unplugging of cables. A yellow triangle appears by every hardware element with an alert.

To clear them, from the Port List tab in Element Manager, right-click anywhere. The pop-up menu in Figure 2-297 displays.


Franz_6C/DC - MCDATA Intrepid
Product Configure Security Logs Maintenance Help
Intrepid 6140
Hardware Port List Node List Performance
Port Properties
Node Properties
Port Optics
☐ Block Port
☐ Enable Beaconing
Port Diagnostics
Port Swapping
Clear Link Incident Alert(s)...
Reset Port
Port Binding
Clear Threshold Alert(s)...

IP Address 10.1.9.2

Domain ID 6C(0C)

Status Fully

State Online

Port #	FC Address	Name	Block Config	State	Type	Operating Speed (Gb/s)	Alert
98	6C6613		Unblocked	Online	F	4 Burst	
99	6C6713		Unblocked	Online	F	4 Burst	
100	6C6813		Unblocked	Online	F	4 Burst	
101	6C6913		Unblocked	Online	F	4 Burst	
102	__6A__		Unblocked	No Light	F	Not Established	
103	6C6B13		Unblocked	Online	F	4 Burst	⚠
104	6C6C13		Unblocked	Online	F	4 Burst	
105	6C6D13		Unblocked	Online	F	4 Burst	
106	6C6E13		Unblocked	Online	F	2	
107	6C6F13		Unblocked	Online	F	2	
108	__70__		Unblocked	Inactive	E		⚠
109	6C7113		Unblocked	Online	F		
110	6C7213		Unblocked	Online	F		
111	6C7313		Unblocked	Online	F		
112	6C7413		Unblocked	Online	F		
113	6C7513		Unblocked	Online	F		
114	6C7613		Unblocked	Online	F		
115	6C7713		Unblocked	Online	F		
116	6C7813		Unblocked	Online	F		
117	6C7913		Unblocked	Online	F		
118	6C7A13		Unblocked	Online	F		
119	6C7B13		Unblocked	Online	F		
120	6C7C13		Unblocked	Online	F		
121	6C7D13		Unblocked	Online	F		

Figure 2-297 Clearing alerts

Now the pop-up menu in Figure 2-298 displays. Select **All Ports on Director**.

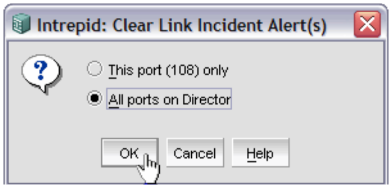

Intrepid: Clear Link Incident Alert(s)
○ This port (108) only
● All ports on Director
OK
Cancel
Help

Figure 2-298 Clearing all ports

2.26.19 Blocking and unblocking ports

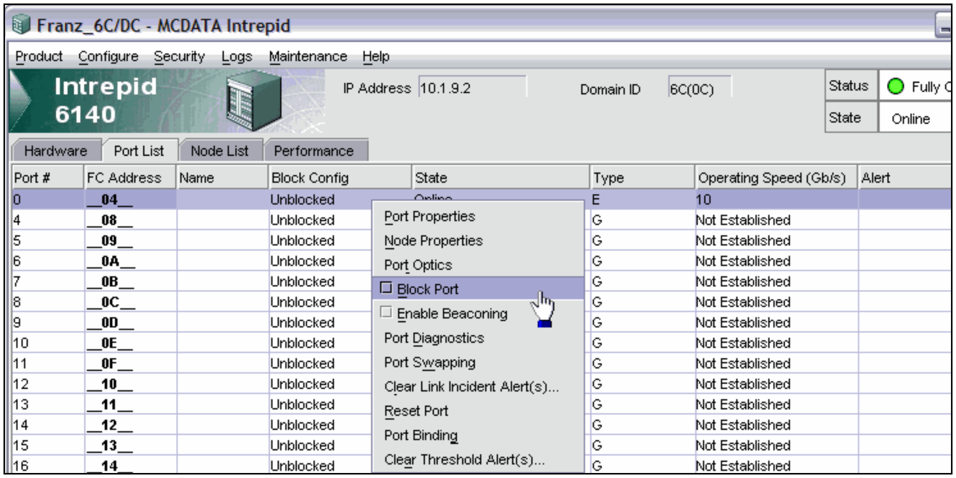
Frequently, new cabling, fabric parameter changes, changes to the node port, and other scenarios, require ports to log back into the fabric. Blocking a port causes light to be dropped and subsequently unblocking the port presents light and causes the attached node to re-log back in. Blocking, then unblocking, ports is the most common cure for problems. For many people, it has become a standard practice to try this before anything else.

Attention: Blocking a port drops all connectivity to everything attached to that port. In mainframe environments, channels connected to the port to be blocked or channels with paths defined to a device connected to a port about to be blocked are typically configured offline before blocking the port.

When a channel is configured offline, light is turned off on that channel interface. The channel does not log back in until the CHPID is configured back online.

Do *not* block device ports. Some devices are known to have problems and require a reboot after blocking the ports at the device. The Intrepid directors reliably block and unblock ports.

From Port List select the port, right-click, and the pop-up menu in Figure 2-299 displays.


Franz_6C/DC - MCDATA Intrepid
Product
Configure
Security
Logs
Maintenance
Help
Intrepid 6140
Hardware
Port List
Node List
Performance
Port Properties
Node Properties
Port Optics
☐ Block Port
☐ Enable Beaconing
Port Diagnostics
Port Swapping
Clear Link Incident Alert(s)...
Reset Port
Port Binding
Clear Threshold Alert(s)...

IP Address 10.1.9.2

Domain ID 6C(0C)

Status Fully

State Online

Port #	FC Address	Name	Block Config	State	Type	Operating Speed (Gb/s)	Alert
0	__04__		Unblocked	Online	E	10	
4	__08__		Unblocked		G	Not Established	
5	__09__		Unblocked		G	Not Established	
6	__0A__		Unblocked		G	Not Established	
7	__0B__		Unblocked		G	Not Established	
8	__0C__		Unblocked		G	Not Established	
9	__0D__		Unblocked		G	Not Established	
10	__0E__		Unblocked		G	Not Established	
11	__0F__		Unblocked		G	Not Established	
12	__10__		Unblocked		G	Not Established	
13	__11__		Unblocked		G	Not Established	
14	__12__		Unblocked		G	Not Established	
15	__13__		Unblocked		G	Not Established	
16	__14__		Unblocked		G	Not Established	

Figure 2-299 Blocking port

Check to block or unblock the port. A warning pop-up menu displays.

2.26.20 Data collection

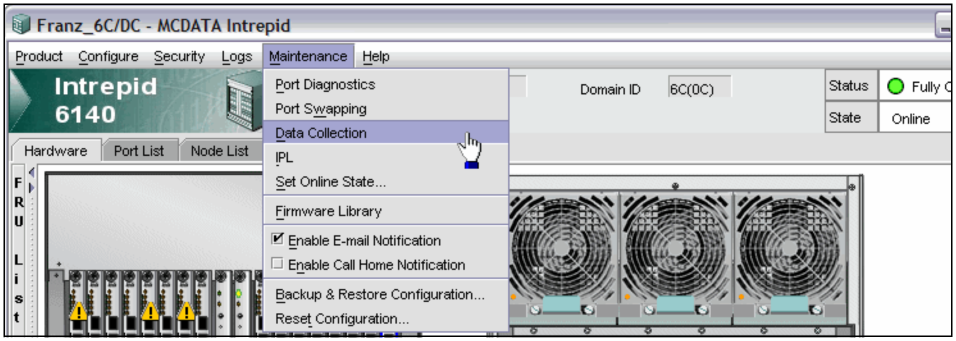
When seeking help with a problem, you will probably be asked to provide the following information:

- A data collection on each director. This is done from the **Maintenance** tab on the element manager.
- IOCDS deck. This comes from the client's system programmer. The IOCDS deck can be generated by selecting **Build I/O Configuration Statements** in HCD.

To get a data collection

If you are taking the data collection from a client, you can just save it to your local disk. The easiest way to get a data collection directly from the server is to plug a USB jump drive into the EFCM server. On EFCM servers shipped from McDATA, the USB ports are located behind the display. Just press on the display where indicated and it should pop open.

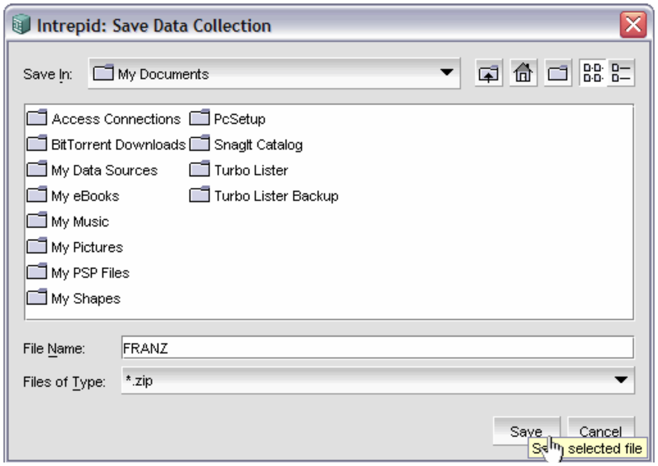
In Element Manager, click **Maintenance** → **Data Collection** as in Figure 2-300.


Franz_6C/DC - MCDATA Intrepid
Product
Configure
Security
Logs
Maintenance
Help
Intrepid 6140
Hardware
Port List
Node List
FRU List
Port Diagnostics
Port Swapping
Data Collection
IPL
Set Online State...
Firmware Library
☑ Enable E-mail Notification
☐ Enable Call Home Notification
Backup & Restore Configuration...
Reset Configuration...
Status
Fully
State
Online

Domain ID 6C(0C)

Figure 2-300 Data collection

The pop-up menu in Figure 2-301 displays.


Intrepid: Save Data Collection
Save In:
My Documents
Access Connections
BitTorrent Downloads
My Data Sources
My eBooks
My Music
My Pictures
My PSP Files
My Shapes
PcSetup
SnagIt Catalog
Turbo Lister
Turbo Lister Backup
Save
Cancel
Save selected file

File Name: FRANZ

Files of Type: *.zip

Figure 2-301 Save data collection

Choose an appropriate file name and location to save the data collection.

2.26.21 Loading firmware

To load firmware select **Maintenance** →**Firmware Library** as in Figure 2-302.

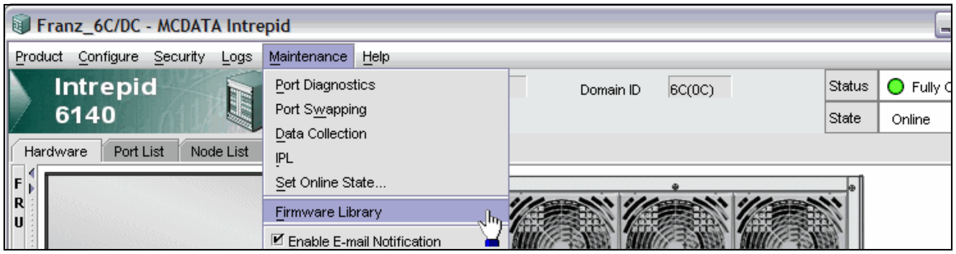
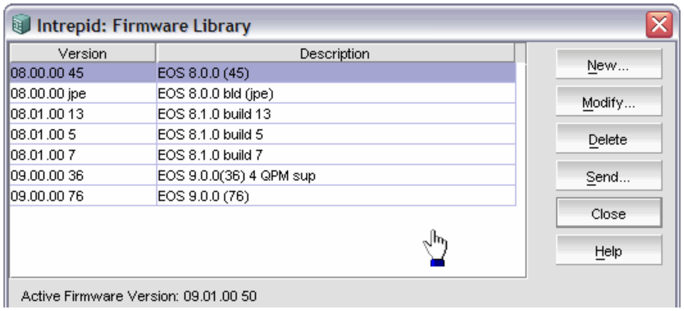

Franz_6C/DC - MCDATA Intrepid
Product
Configure
Security
Logs
Maintenance
Help
Intrepid 6140
Hardware
Port List
Node List
FRU
Port Diagnostics
Port Swapping
Data Collection
IPL
Set Online State...
Firmware Library
Enable E-mail Notification
Domain ID
6C(0C)
Status
Fully C
State
Online

Figure 2-302 Firmware library

The firmware library displays as in Figure 2-303.


Intrepid: Firmware Library
New...
Modify...
Delete
Send...
Close
Help

Version	Description
08.00.00 45	EOS 8.0.0 (45)
08.00.00 jpe	EOS 8.0.0 bld (jpe)
08.01.00 13	EOS 8.1.0 build 13
08.01.00 5	EOS 8.1.0 build 5
08.01.00 7	EOS 8.1.0 build 7
09.00.00 36	EOS 9.0.0(36) 4 QPM sup
09.00.00 76	EOS 9.0.0 (76)

Active Firmware Version: 09.01.00 50

Figure 2-303 Selecting firmware

2.26.22 Back up and restore configuration

To back up and restore the configuration, select **Maintenance** →**Backup & Restore Configuration** from Element Manager as in Figure 2-304.

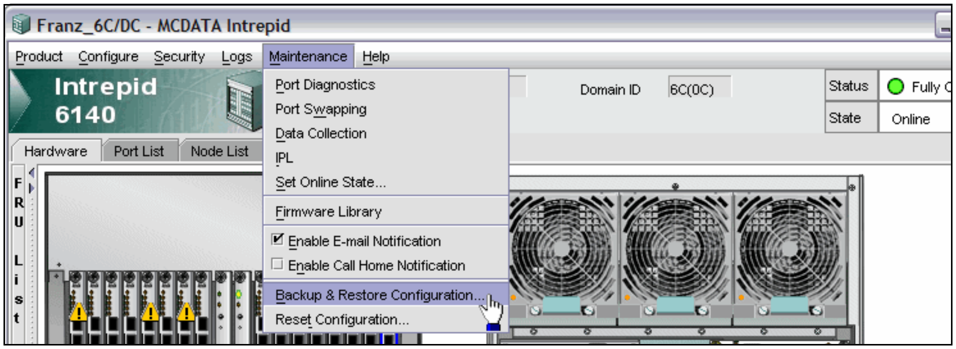
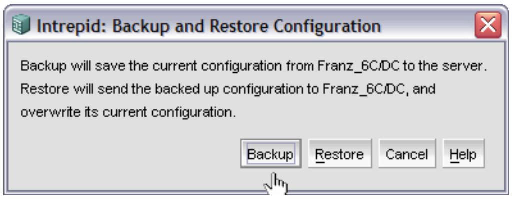

Franz_6C/DC - MCDATA Intrepid
Product
Configure
Security
Logs
Maintenance
Help
Intrepid
6140
Hardware
Port List
Node List
FRU List
Port Diagnostics
Port Swapping
Data Collection
IPL
Set Online State...
Firmware Library
Enable E-mail Notification
Enable Call Home Notification
Backup & Restore Configuration...
Reset Configuration...
Domain ID
6C(0C)
Status
Fully
State
Online

Figure 2-304 Backup and restore

The pop-up menu in Figure 2-305 displays.


Intrepid: Backup and Restore Configuration
Backup
Restore
Cancel
Help

Backup will save the current configuration from Franz_6C/DC to the server. Restore will send the backed up configuration to Franz_6C/DC, and overwrite its current configuration.

Figure 2-305

Click **Backup** to back up the configuration. To restore a previously saved configuration, click **Restore**.

3

Implementing a SAN with the q-type family

For less complex SAN environments, with fewer servers and storage arrays, a single switch or dual cascaded switches offer redundancy and performance with minimal administration and lower cost than larger directors. One option for these smaller infrastructures is an entry-level switch such as the IBM TotalStorage Storage Switch SAN10Q-2, which offers edge switch capability with full 4Gbps port speed.

Note: The SAN10Q-2 also has a command line interface (CLI). In this chapter we are using the GUI to perform our implementation. For details of the CLI, refer to the following User's Guide:

System Storage SAN10Q 4 Gbps 10-Port Fibre Channel SwitchType 6918 User's Guide, 31R1632

© Copyright IBM Corp. 1999-2007. All rights reserved.

3.1 Introducing the IBM TotalStorage Switch SAN10Q-2

The IBM TotalStorage Storage Switch SAN10Q-2 is an affordable, capable, and extremely easy to use, entry-level IBM System. The SAN10Q-2 is a one-half width, 1U rack height, ten-port 4Gb switch as shown in Figure 3-1. This switch provides the following features:

- Throughput of 1, 2, or 4 gigabits per second on all ports, short wave, and long wave
- Single E port support for the inclusion of another IBM System Storage SAN10Q-2 for redundancy or extension of SAN to larger fabric
- Hardware-enforced zoning helps protect against non-secure, unauthorized and unauthenticated network and management access and World Wide Name spoofing
- Hot-pluggable optical transceivers that can be replaced without taking switch offline
- All firmware included, and no additional license keys required
- Per-port buffering: ASIC-embedded memory (non-shared) and 8-credit zero wait for each port

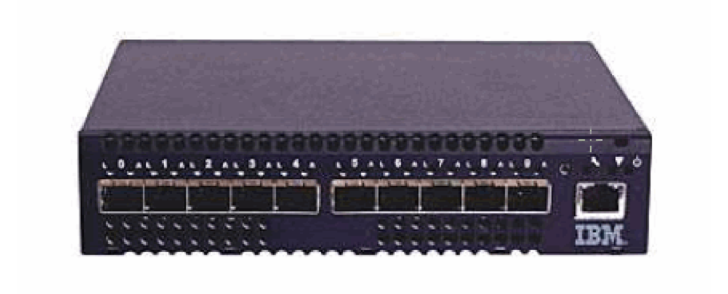


Figure 3-1 IBM TotalStorage Storage Switch SAN10Q-2

More option and pricing information on the TotalStorage Switch SAN10Q-2 can be found on the IBM storage Web site at:

`http://www-03.ibm.com/servers/storage/san/q_type/san10q/`

3.2 Installation

The items shown in Figure 3-2 all are supplied with the SAN10Q switch. The Support and Documentation CD contains all documentation and software required to install and setup the switch.

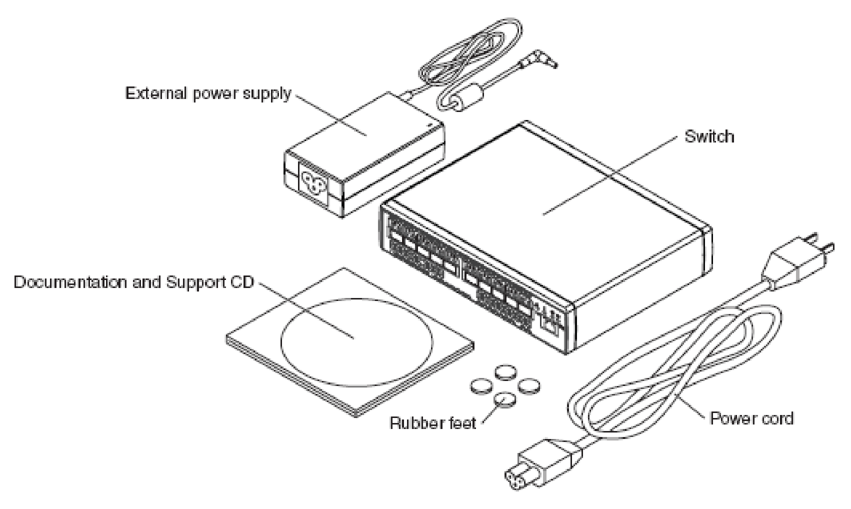
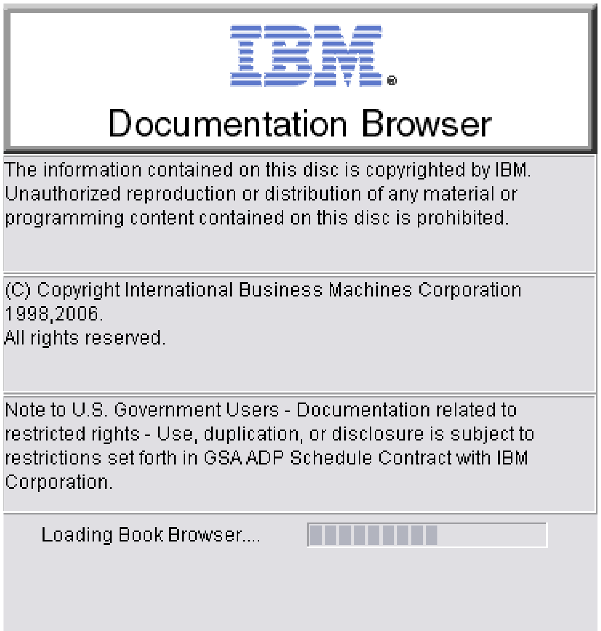

External power supply
Switch
Documentation and Support CD
Rubber feet
Power cord

Figure 3-2 SAN10Q

3.2.1 Documentation

All documentation is on the supplied CD. In the following topics, we explain how to install the CD so you can read the documentation.

Autostart is enabled by default on your CD drive. Upon insertion of the CD, you should see the display in Figure 3-3. If autostart is disabled on the workstation, then click **Start** → **Run**, at the **C>** prompt, then type **H:\win32.bat**, where H is the drive letter of the CD drive on this workstation.



The information contained on this disc is copyrighted by IBM. Unauthorized reproduction or distribution of any material or programming content contained on this disc is prohibited.

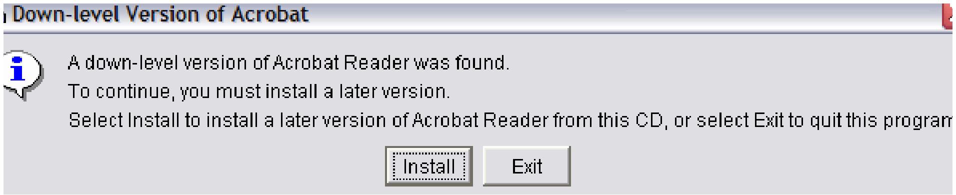
(C) Copyright International Business Machines Corporation 1998,2006.
All rights reserved.

Note to U.S. Government Users - Documentation related to restricted rights - Use, duplication, or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corporation.

Loading Book Browser....

Figure 3-3 Document Browser setup

If you do not have Acrobat® reader V5, you must install Acrobat reader now. When you receive the message shown in Figure 3-4, click the **Install** button.

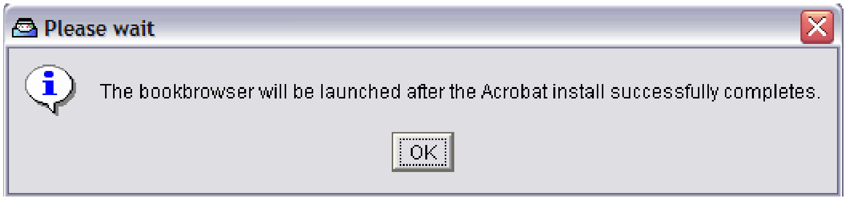


A down-level version of Acrobat Reader was found.
To continue, you must install a later version.
Select Install to install a later version of Acrobat Reader from this CD, or select Exit to quit this program

Figure 3-4 Acrobat Installation warning

> **Note:** If you have a higher version of Acrobat, such as version 5.1 or higher installed, you are still required to click the **Install** button to continue.

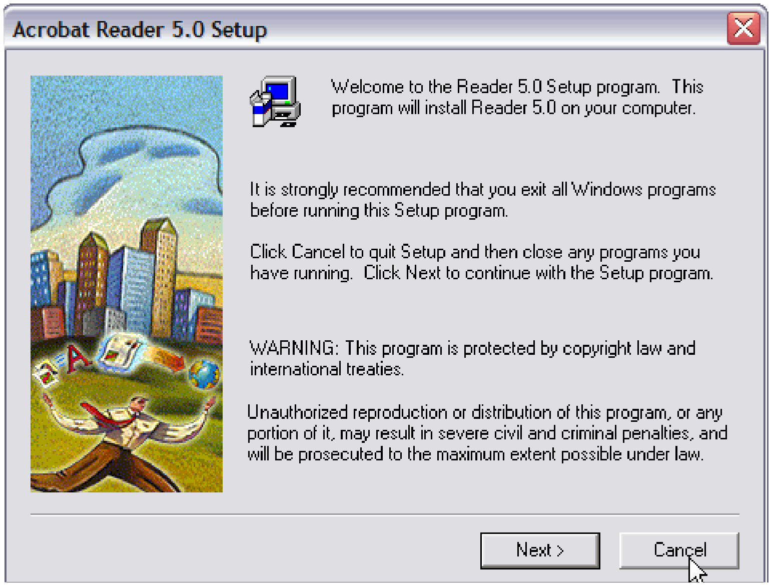
Click the **OK**, button, shown in Figure 3-5, to continue with the installation.



The bookbrowser will be launched after the Acrobat install successfully completes.

Figure 3-5 Status display

Next, as shown in Figure 3-6, you have to make a decision of either cancelling the Acrobat install or continuing.



Welcome to the Reader 5.0 Setup program. This program will install Reader 5.0 on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

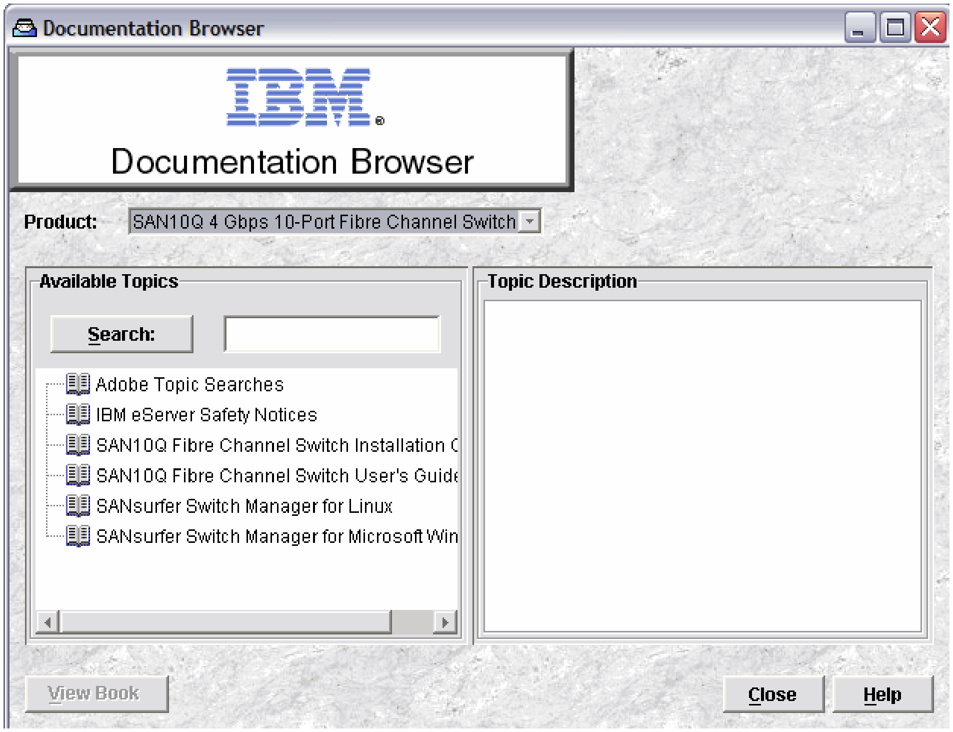
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Figure 3-6 Acrobat installation window.

If you have Acrobat reader V5.1 or higher already installed on your workstation, click the **Cancel** button now.

If you do not have Acrobat installed, or if you have a version lower than V5.0, then click the **Next** button and continue to install Acrobat.

When the installation of Acrobat is finished, or if you cancelled the installation of Acrobat, you get the Document Browser window displayed, as shown in Figure 3-7. All documentation required for installation and operation can be accessed from this window.


Documentation Browser
IBM
Documentation Browser
Available Topics
Search:
Adobe Topic Searches
IBM eServer Safety Notices
SAN10Q Fibre Channel Switch Installation C
SAN10Q Fibre Channel Switch User's Guide
SANsurfer Switch Manager for Linux
SANsurfer Switch Manager for Microsoft Win
Topic Description
View Book
Close
Help

Product: SAN10Q 4 Gbps 10-Port Fibre Channel Switch

Figure 3-7 Document Browser

3.2.2 Installing SANsurfer Switch Manager

In Table 3-1 we show the SANsurfer workstation requirements.

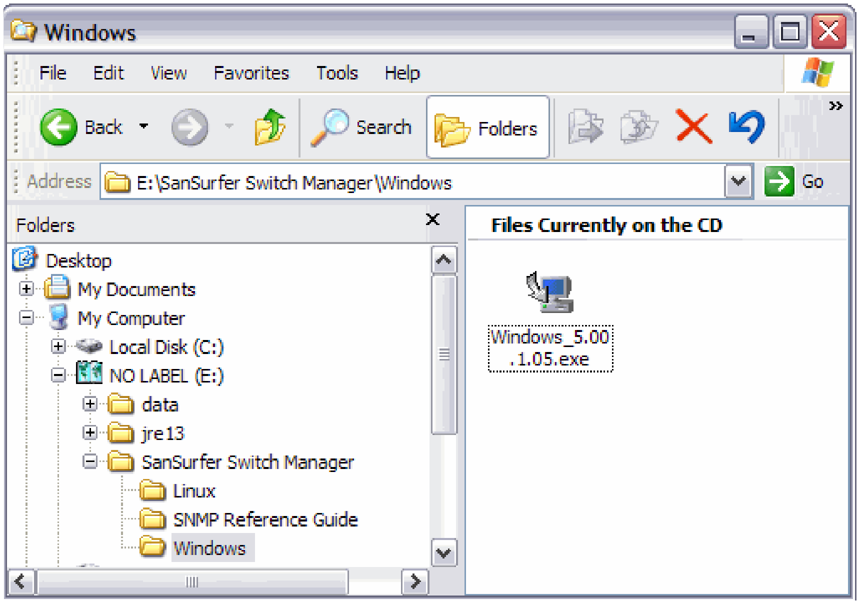
Table 3-1 SANsurfer workstation requirements

Component	Requirements
Operating system	▸ Microsoft Windows 2000,2003 and Windows XP ▸ Red Hat Enterprise Linux Version 3 or later ▸ SUSE Linux Enterprise Server 9.0
Memory	256 MB or more
Disk space	150 MB per installation
Processor	500 MHz or faster
Hardware	CD drive, RJ-45 Ethernet port

Component	Requirements
Internet browser	► Microsoft Internet Explorer 5.0 or later ► Netscape Navigator 4.72 or later ► Mozilla 1.02 or later ► Java 2 Run Time Environment to support the WEB applet

Next we show an example of how to install SANsurfer switch manager using a Windows XP operating system.

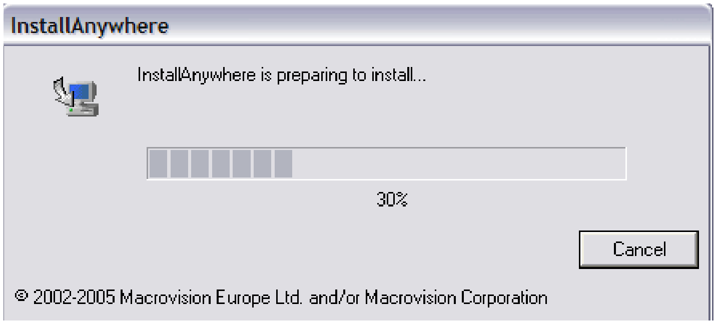
Explore the CD and from the root directory, click the *SANsurfer Switch Manager* folder. Read the readme file and the release notes. From the *Windows* folder, double-click Windows_5.00.1.05.exe, as shown in Figure 3-8.


Windows
File
Edit
View
Favorites
Tools
Help
Back
Search
Folders
Address
Go
Folders
Desktop
My Documents
My Computer
Local Disk (C:)
NO LABEL (E:)
data
jre13
SanSurfer Switch Manager
Linux
SNMP Reference Guide
Windows
Files Currently on the CD
Windows_5.00.1.05.exe

Address: E:\SanSurfer Switch Manager\Windows

Figure 3-8 Switch Manager directory on CD

The install program now starts, and you see a progress window as shown in Figure 3-9.


InstallAnywhere
Cancel

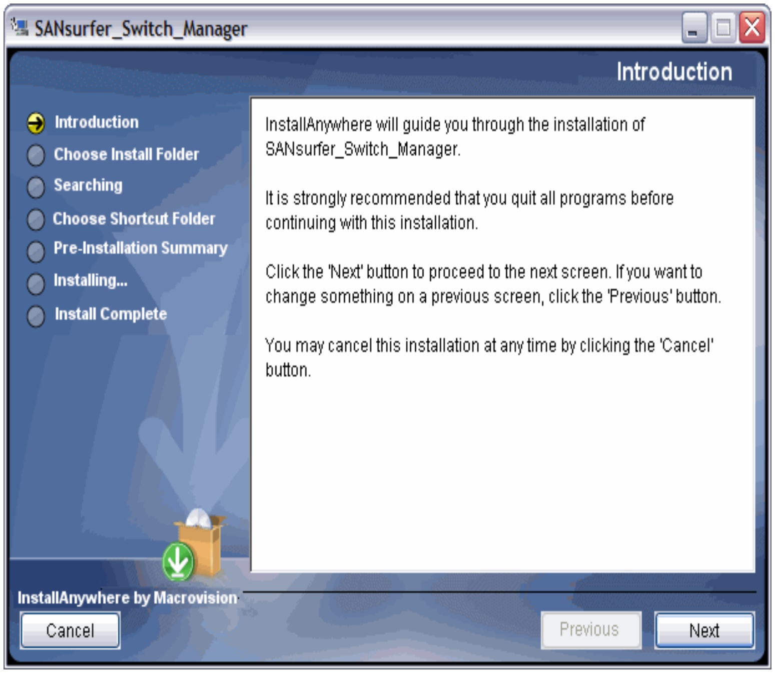
InstallAnywhere is preparing to install...

30%

© 2002-2005 Macrovision Europe Ltd. and/or Macrovision Corporation

Figure 3-9 Preparing to install

Read the introduction window, shown in Figure 3-10, and click the **Next** button on this window.


SANsurfer_Switch_Manager
Introduction
Introduction
Choose Install Folder
Searching
Choose Shortcut Folder
Pre-Installation Summary
Installing...
Install Complete
InstallAnywhere by Macrovision
Cancel
Previous
Next

InstallAnywhere will guide you through the installation of SANsurfer_Switch_Manager.

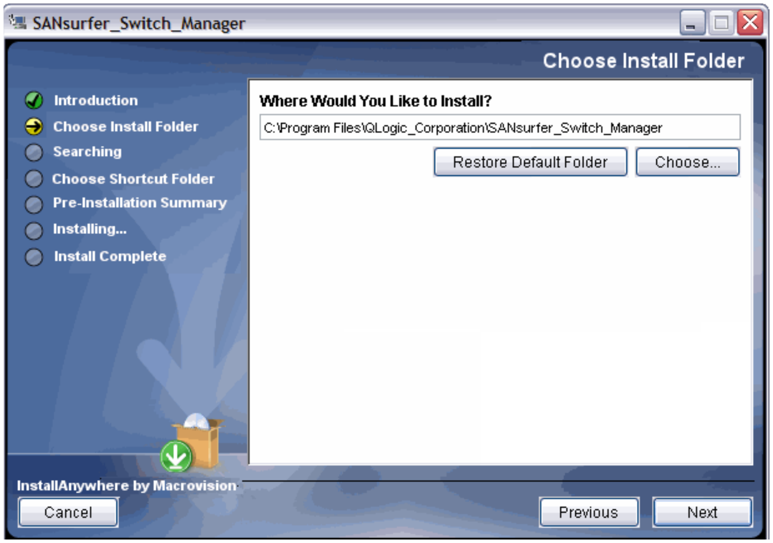
It is strongly recommended that you quit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

Figure 3-10 Switch Manager Introduction

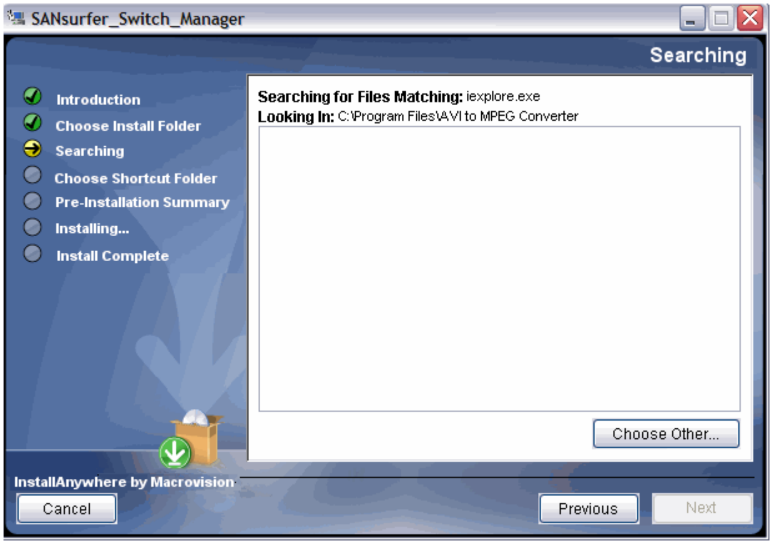
Now choose the folder where you wish to install Switch Manager, or select the default, and click the **Next** button, as shown in Figure 3-11.


SANsurfer_Switch_Manager
Choose Install Folder
Introduction
Choose Install Folder
Searching
Choose Shortcut Folder
Pre-Installation Summary
Installing...
Install Complete
Restore Default Folder
Choose...
InstallAnywhere by Macrovision
Cancel
Previous
Next

Where Would You Like to Install?
C:\Program Files\QLogic_Corporation\SANsurfer_Switch_Manager

Figure 3-11 Switch Manager install folder

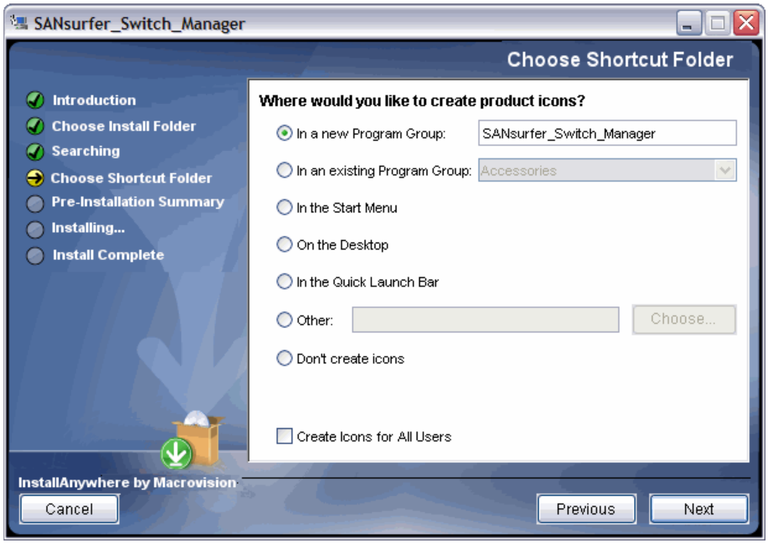
The install process now checks your installed software for compatibility, as shown in Figure 3-12.


SANsurfer_Switch_Manager
Searching
Introduction
Choose Install Folder
Searching
Choose Shortcut Folder
Pre-Installation Summary
Installing...
Install Complete
Choose Other...
InstallAnywhere by Macrovision
Cancel
Previous
Next

Searching for Files Matching: iexplore.exe
Looking In: C:\Program Files\AVI to MPEG Converter

Figure 3-12 Checking software

You are now given the option of where to create the icon for Switch Manager, as shown in Figure 3-13. Select your option and click **Next**.


SANsurfer_Switch_Manager
Choose Shortcut Folder
Introduction
Choose Install Folder
Searching
Choose Shortcut Folder
Pre-Installation Summary
Installing...
Install Complete
InstallAnywhere by Macrovision
Cancel
Previous
Next

Where would you like to create product icons?

● In a new Program Group: SANsurfer_Switch_Manager

○ In an existing Program Group: Accessories

○ In the Start Menu

○ On the Desktop

○ In the Quick Launch Bar

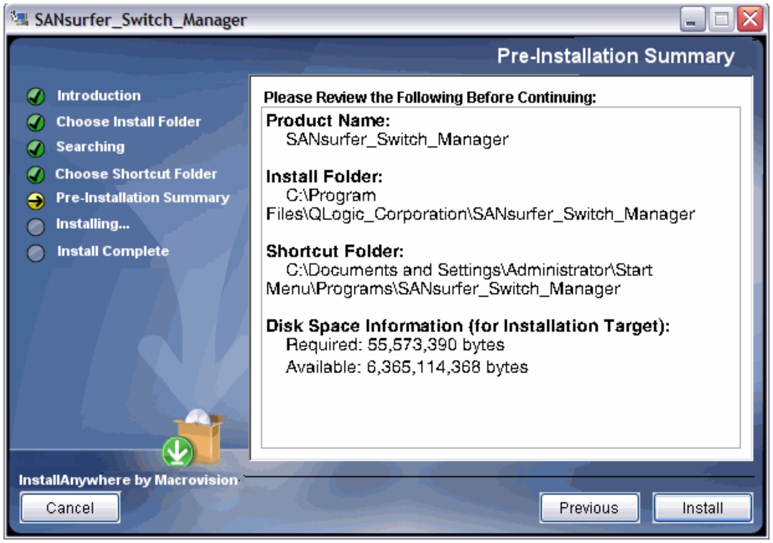
○ Other: Choose...

○ Don't create icons

☐ Create Icons for All Users

Figure 3-13 Selecting icon preference

You get to review details regarding the installation, shown in Figure 3-14. To continue, click **Install**.


SANsurfer_Switch_Manager
Pre-Installation Summary
Introduction
Choose Install Folder
Searching
Choose Shortcut Folder
Pre-Installation Summary
Installing...
Install Complete
InstallAnywhere by Macrovision
Cancel
Previous
Install

Please Review the Following Before Continuing:

Product Name:
SANsurfer_Switch_Manager

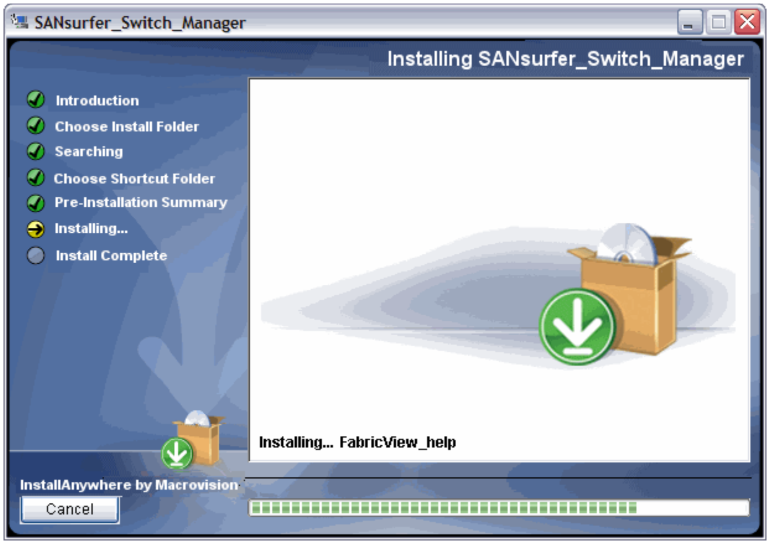
Install Folder:
C:\Program Files\QLogic_Corporation\SANsurfer_Switch_Manager

Shortcut Folder:
C:\Documents and Settings\Administrator\Start Menu\Programs\SANsurfer_Switch_Manager

Disk Space Information (for Installation Target):
Required: 55,573,390 bytes
Available: 6,365,114,368 bytes

Figure 3-14 Installation review

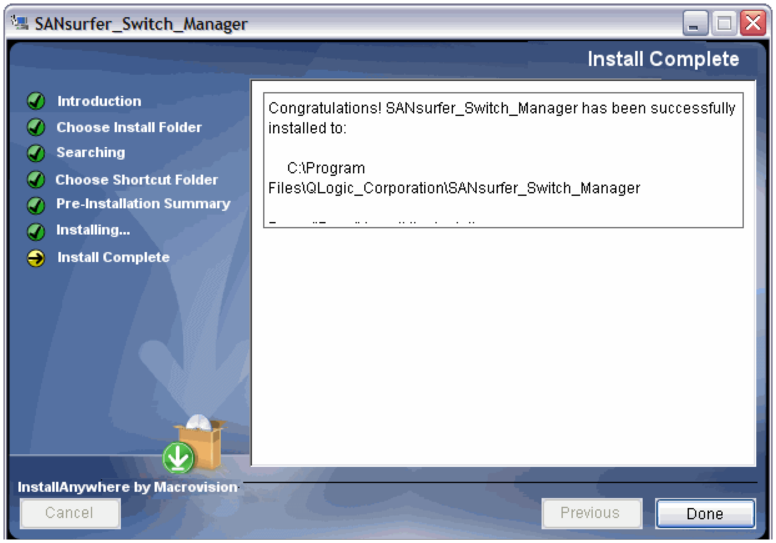
SANsurfer Switch Manager is now being installed, as shown in the progress window in Figure 3-15. This takes a few minutes.


SANsurfer_Switch_Manager
Installing SANsurfer_Switch_Manager
Introduction
Choose Install Folder
Searching
Choose Shortcut Folder
Pre-Installation Summary
Installing...
Install Complete
InstallAnywhere by Macrovision
Cancel

Installing... FabricView_help

Figure 3-15 Switch Manager installation

Figure 3-16 shows that installation is complete.


SANsurfer_Switch_Manager
Install Complete
Introduction
Choose Install Folder
Searching
Choose Shortcut Folder
Pre-Installation Summary
Installing...
Install Complete
InstallAnywhere by Macrovision
Cancel
Previous
Done

Congratulations! SANsurfer_Switch_Manager has been successfully installed to:

C:\Program Files\QLogic_Corporation\SANsurfer_Switch_Manager

Figure 3-16 SANsurfer Switch Manager installation complete

This completes the installation of SANsurfer Switch Manager. You can launch this application from your Start Program menu, or the icon on your desktop.

3.2.3 Installing the Fibre Channel switch

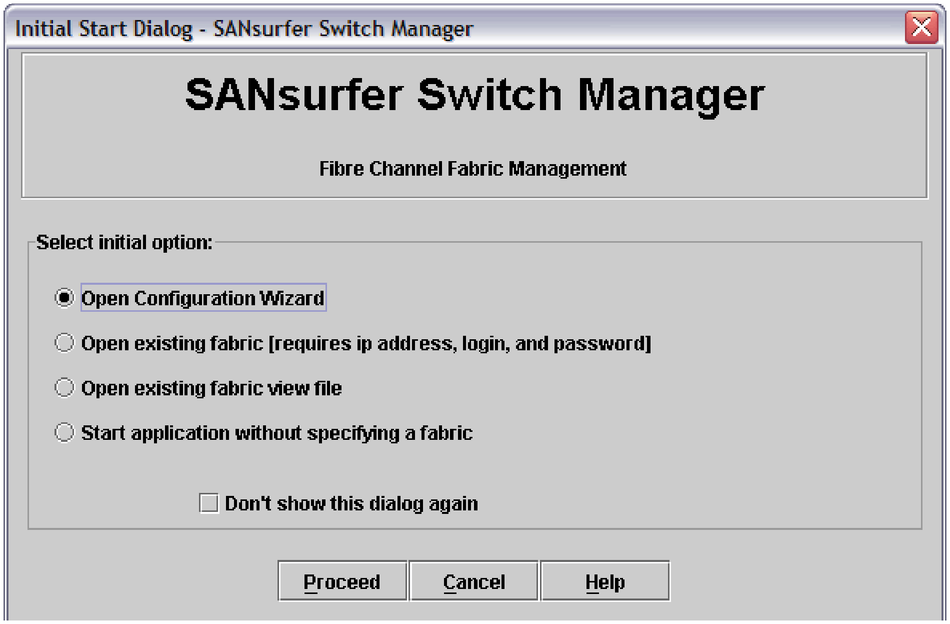
In this topic we describe how to install the switch:

- Connect the new switch to the external power supply, and plug in the line cord to the power supply.
- Install either a standard RJ-45 ethernet cable from the SAN10Q to the management network, or a cross over RJ-45 ethernet cable to your work station where you have installed SANsurfer.
- Obtain the IP address that you intend to use on the SAN10Q switch.
- Make sure your workstation’s ethernet port is set up in the same IP subnet as the required switch address.
- Start SANsurfer Switch Manager on your workstation.

Start up SANsurfer using the icon on your desktop, Figure 3-17, or from your program list.

Figure 3-17 Start SANsurfer

From the Initial Start Dialog window, Figure 3-18, select the **Open Configuration Wizard** button and select **Proceed**.


Initial Start Dialog - SANsurfer Switch Manager
SANsurfer Switch Manager
Fibre Channel Fabric Management
Proceed
Cancel
Help

Select initial option:

● Open Configuration Wizard

○ Open existing fabric [requires ip address, login, and password]

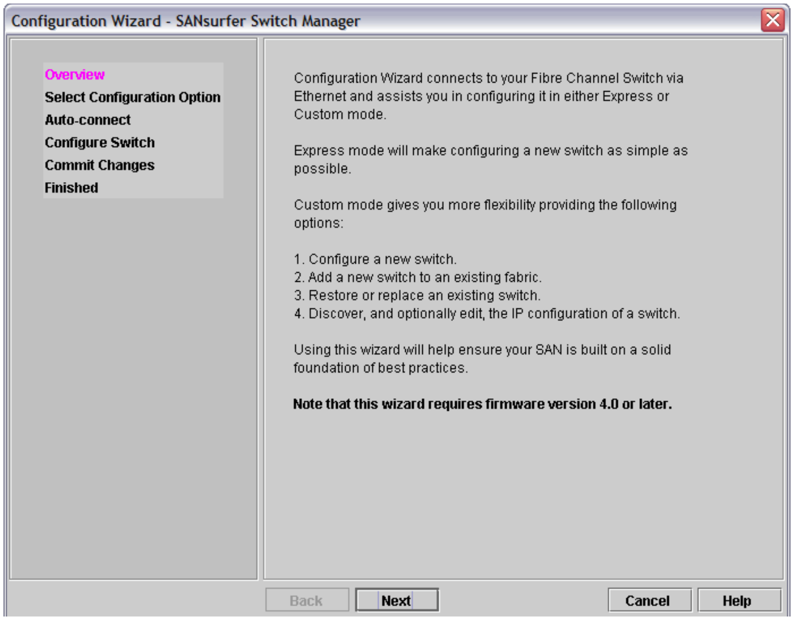
○ Open existing fabric view file

○ Start application without specifying a fabric

☐ Don't show this dialog again

Figure 3-18 SANsurfer Initial Start Dialog window.

Read the overview window, Figure 3-19, and select **Next**.


Configuration Wizard - SANsurfer Switch Manager
Overview
Select Configuration Option
Auto-connect
Configure Switch
Commit Changes
Finished
Back
Next
Cancel
Help

Configuration Wizard connects to your Fibre Channel Switch via Ethernet and assists you in configuring it in either Express or Custom mode.

Express mode will make configuring a new switch as simple as possible.

Custom mode gives you more flexibility providing the following options:

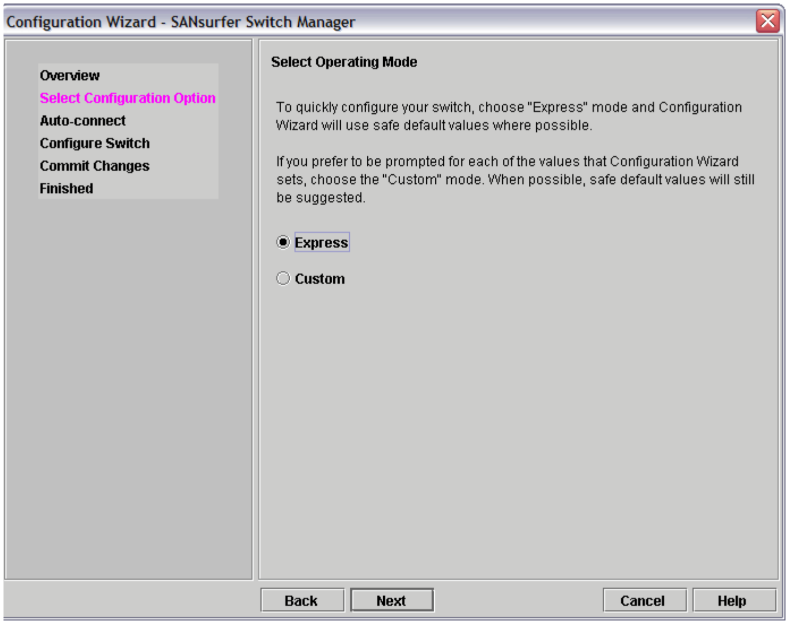
1. Configure a new switch.
2. Add a new switch to an existing fabric.
3. Restore or replace an existing switch.
4. Discover, and optionally edit, the IP configuration of a switch.

Using this wizard will help ensure your SAN is built on a solid foundation of best practices.

Note that this wizard requires firmware version 4.0 or later.

Figure 3-19 Configuration Wizard overview

Select the **Express** option from the Select Configuration Option window, Figure 3-20 and then select **Next**.



Configuration Wizard - SANsurfer Switch Manager
Overview
Select Configuration Option
Auto-connect
Configure Switch
Commit Changes
Finished

Select Operating Mode

To quickly configure your switch, choose "Express" mode and Configuration Wizard will use safe default values where possible.

If you prefer to be prompted for each of the values that Configuration Wizard sets, choose the "Custom" mode. When possible, safe default values will still be suggested.

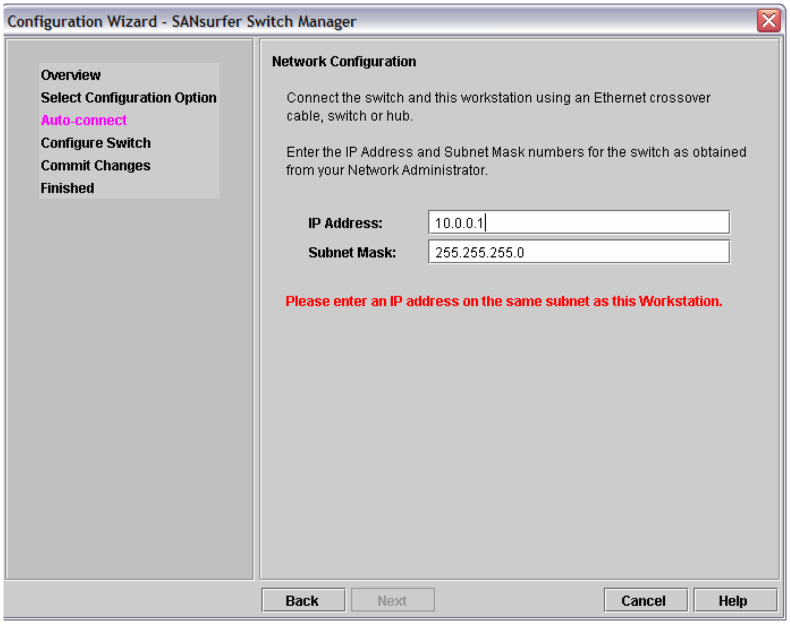
● Express

○ Custom

Back
Next
Cancel
Help

Figure 3-20 Configuration Wizard selection window

In the Network Configuration window, enter the IP address and subnet mask you wish to configure on the new switch. The wizard checks to make sure the subnet you enter is on the same subnet that is configured on your workstation’s local ethernet interface. If not, you cannot continue, and a warning message is displayed as shown in Figure 3-21.


Configuration Wizard - SANsurfer Switch Manager
Overview
Select Configuration Option
Auto-connect
Configure Switch
Commit Changes
Finished
Back
Next
Cancel
Help

Network Configuration

Connect the switch and this workstation using an Ethernet crossover cable, switch or hub.

Enter the IP Address and Subnet Mask numbers for the switch as obtained from your Network Administrator.

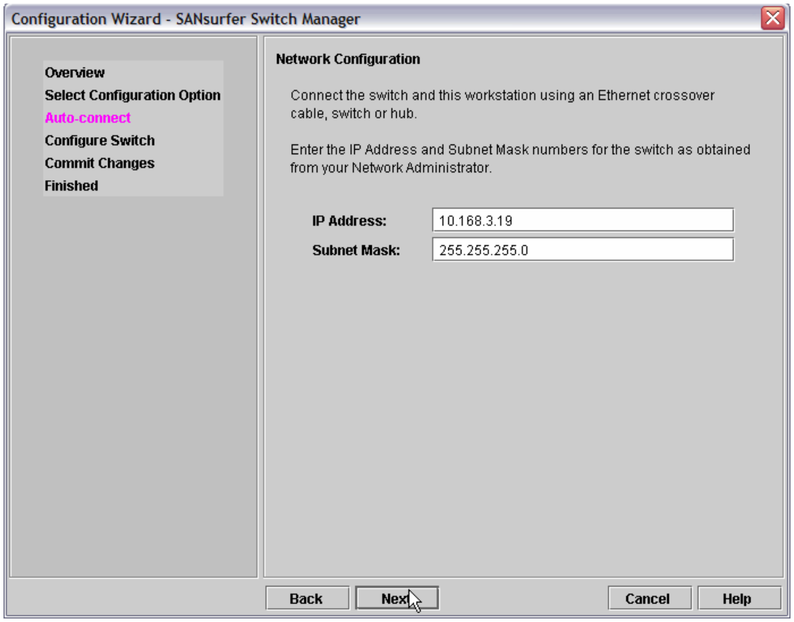
IP Address: 10.0.0.1

Subnet Mask: 255.255.255.0

Please enter an IP address on the same subnet as this Workstation.

Figure 3-21 Configuration Wizard Network Configuration warning window

Enter the correct IP address information as shown in Figure 3-22 and select **Next**.


Configuration Wizard - SANsurfer Switch Manager
Overview
Select Configuration Option
Auto-connect
Configure Switch
Commit Changes
Finished
Back
Next
Cancel
Help

Network Configuration

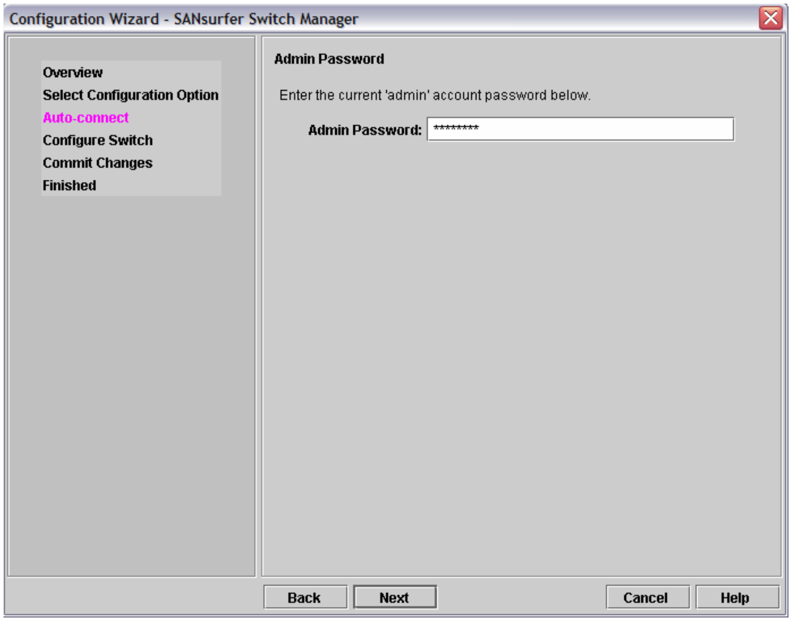
Connect the switch and this workstation using an Ethernet crossover cable, switch or hub.

Enter the IP Address and Subnet Mask numbers for the switch as obtained from your Network Administrator.

IP Address: 10.168.3.19
Subnet Mask: 255.255.255.0

Figure 3-22 Configuration Wizard Network Configuration window

The default password for the *admin* user is *password*. Enter this information in the Auto-connect window, Figure 3-22, and select **Next**.


Configuration Wizard - SANsurfer Switch Manager
Overview
Select Configuration Option
Auto-connect
Configure Switch
Commit Changes
Finished
Back
Next
Cancel
Help

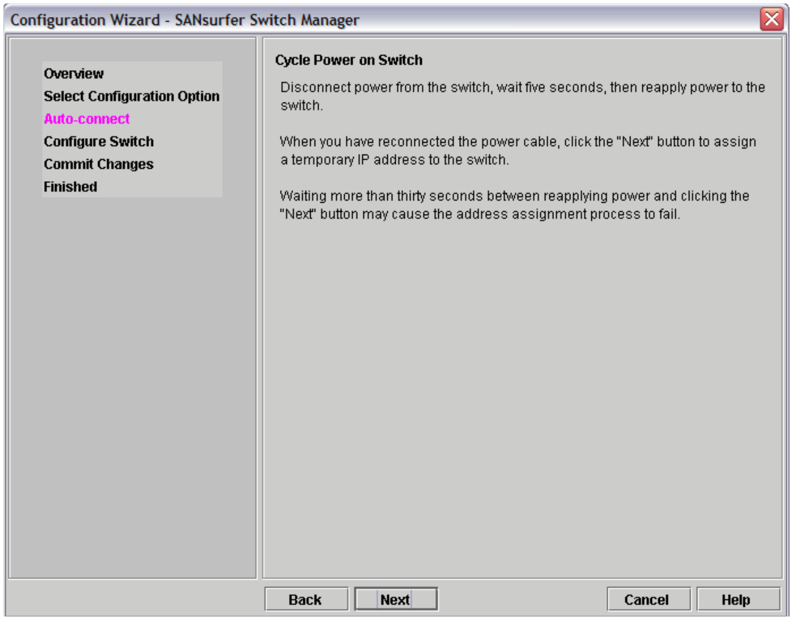
Admin Password

Enter the current 'admin' account password below.

Admin Password: ********

Figure 3-23 Configuration Wizard Auto-connect window

Follow the on-screen instructions as shown in Figure 3-24, and select **Next**.


Configuration Wizard - SANsurfer Switch Manager
Overview
Select Configuration Option
Auto-connect
Configure Switch
Commit Changes
Finished
Back
Next
Cancel
Help

Cycle Power on Switch

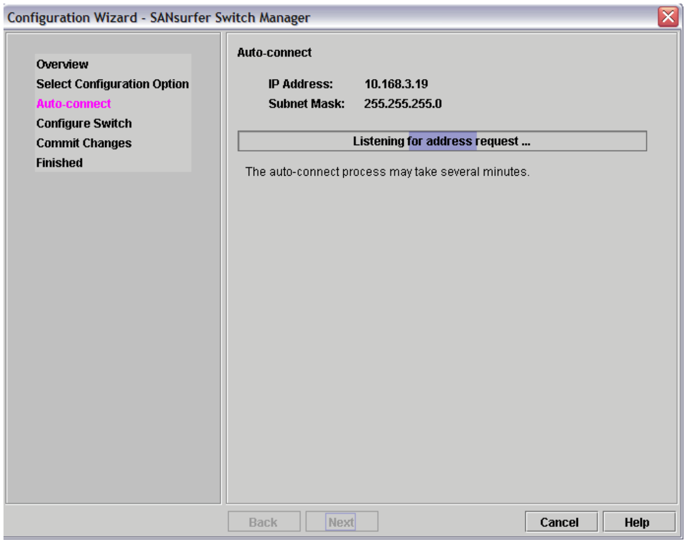
Disconnect power from the switch, wait five seconds, then reapply power to the switch.

When you have reconnected the power cable, click the "Next" button to assign a temporary IP address to the switch.

Waiting more than thirty seconds between reapplying power and clicking the "Next" button may cause the address assignment process to fail.

Figure 3-24 Configuration Wizard Auto connect window

During boot up of the SAN10Q, the window shown in Figure 3-25 is displayed.


Configuration Wizard - SANsurfer Switch Manager
Overview
Select Configuration Option
Auto-connect
Configure Switch
Commit Changes
Finished
Back
Next
Cancel
Help

Auto-connect

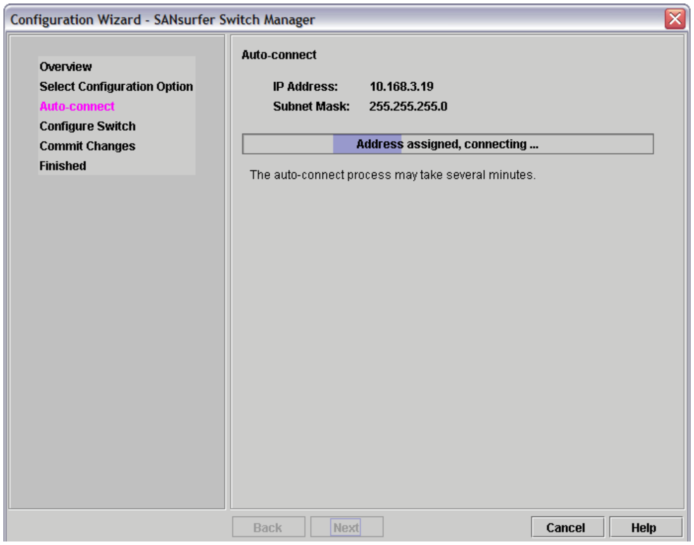
IP Address: 10.168.3.19
Subnet Mask: 255.255.255.0

Listening for address request ...

The auto-connect process may take several minutes.

Figure 3-25 Configuration Wizard status window

When the switch has booted, it sends a request for an IP address to SANsurfer. SANsurfer then assigns the switch the IP address you configured, as shown in Figure 3-26.


Configuration Wizard - SANsurfer Switch Manager
Overview
Select Configuration Option
Auto-connect
Configure Switch
Commit Changes
Finished
Back
Next
Cancel
Help

Auto-connect

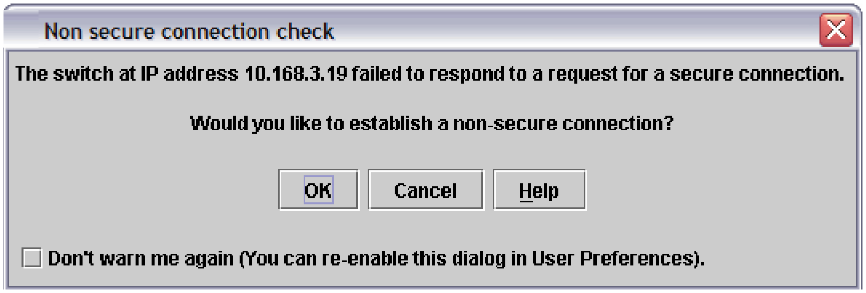
IP Address: 10.168.3.19
Subnet Mask: 255.255.255.0

Address assigned, connecting ...

The auto-connect process may take several minutes.

Figure 3-26 Configuration Wizard IP address setup

You now receive a security warning, due to this being a new installation. Select **OK** to continue (Figure 3-27).


Non secure connection check
OK
Cancel
Help

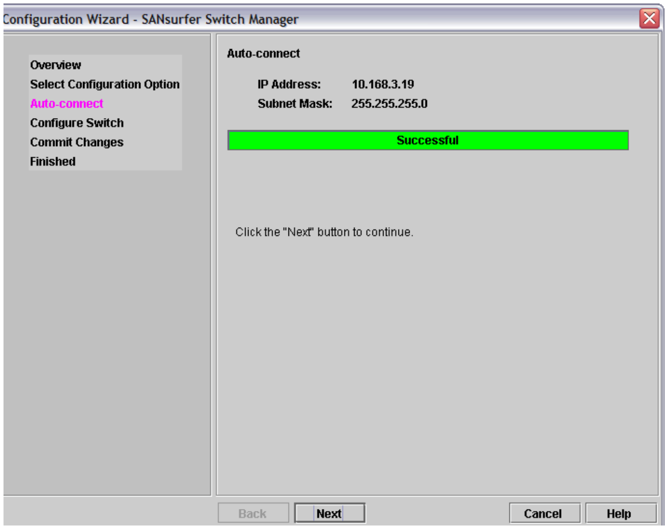
The switch at IP address 10.168.3.19 failed to respond to a request for a secure connection.

Would you like to establish a non-secure connection?

☐ Don't warn me again (You can re-enable this dialog in User Preferences).

Figure 3-27 Security warning

The window shown in Figure 3-28 is displayed when the wizard has successfully configured the IP settings. Select **Next** to continue with switch setup.


Configuration Wizard - SANsurfer Switch Manager
Overview
Select Configuration Option
Auto-connect
Configure Switch
Commit Changes
Finished
Back
Next
Cancel
Help

Auto-connect

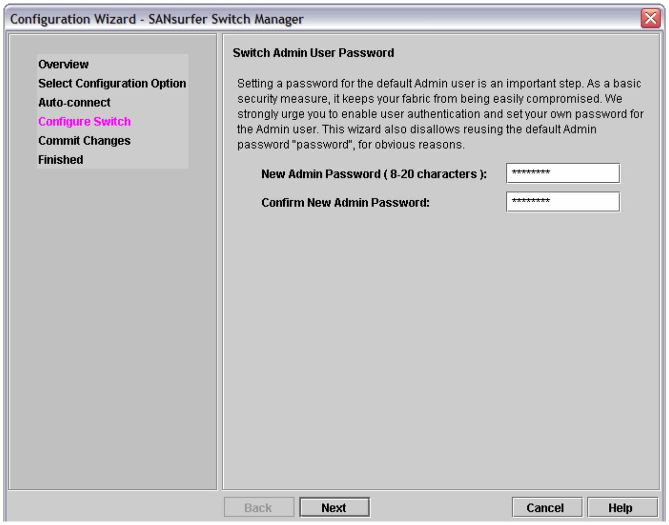
IP Address: 10.168.3.19
Subnet Mask: 255.255.255.0

Successful

Click the "Next" button to continue.

Figure 3-28 Configuration Wizard auto-connect successful

You now have the option to change your *admin* user password. Read the minimum requirements for this password and key it into this window, shown in Figure 3-29. Select **Next** to continue.


Configuration Wizard - SANsurfer Switch Manager
Overview
Select Configuration Option
Auto-connect
Configure Switch
Commit Changes
Finished
Back
Next
Cancel
Help

Switch Admin User Password

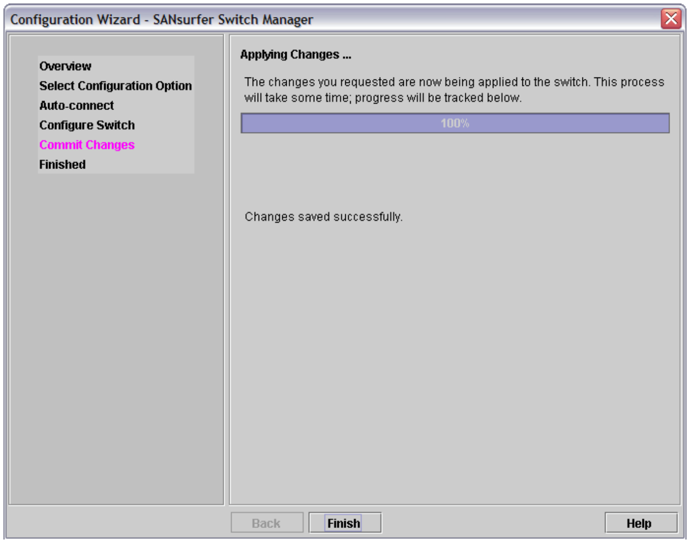
Setting a password for the default Admin user is an important step. As a basic security measure, it keeps your fabric from being easily compromised. We strongly urge you to enable user authentication and set your own password for the Admin user. This wizard also disallows reusing the default Admin password "password", for obvious reasons.

New Admin Password (8-20 characters): ********

Confirm New Admin Password: ********

Figure 3-29 Configuration Wizard change password

You can now monitor the final stage of the setup while SANsurfer applies the changes to your switch as shown in Figure 3-30. Wait for the completion message and select **Finish**.


Configuration Wizard - SANsurfer Switch Manager
Overview
Select Configuration Option
Auto-connect
Configure Switch
Commit Changes
Finished
100%
Back
Finish
Help

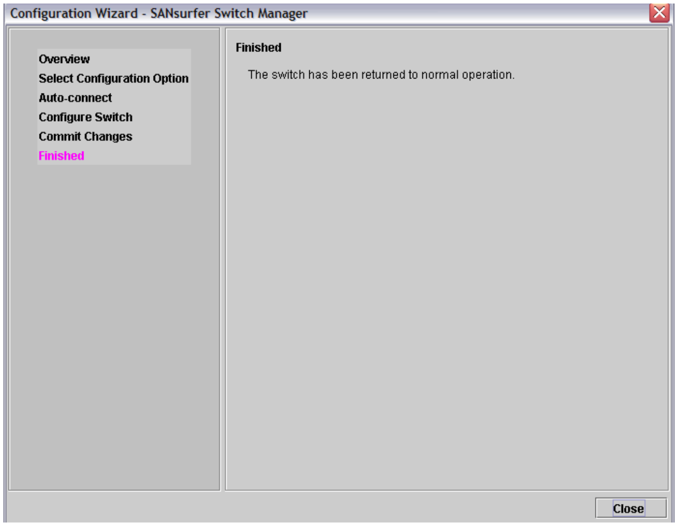
Applying Changes ...

The changes you requested are now being applied to the switch. This process will take some time; progress will be tracked below.

Changes saved successfully.

Figure 3-30 Configuration Wizard applying changes

This completes the initial setup of the switch. Select the **Close** button in Figure 3-31.


Configuration Wizard - SANsurfer Switch Manager

Overview
Select Configuration Option
Auto-connect
Configure Switch
Commit Changes
Finished

Finished

The switch has been returned to normal operation.

Close

Figure 3-31 Configuration Wizard completion.

You are now taken into the initial SANsurfer Switch Manager window, as shown in Figure 3-32.

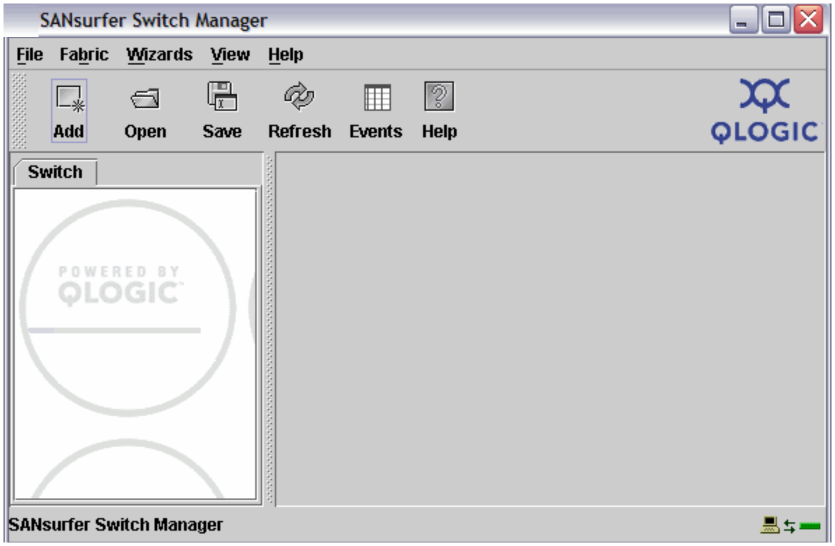

SANsurfer Switch Manager
File
Fabric
Wizards
View
Help
Add
Open
Save
Refresh
Events
Help
QLOGIC
Switch
POWERED BY QLOGIC
SANsurfer Switch Manager

Figure 3-32 SANsurfer Switch Manager initial display

Now select **Fabric** → **Add Fabric** from the main menu; see Figure 3-33.

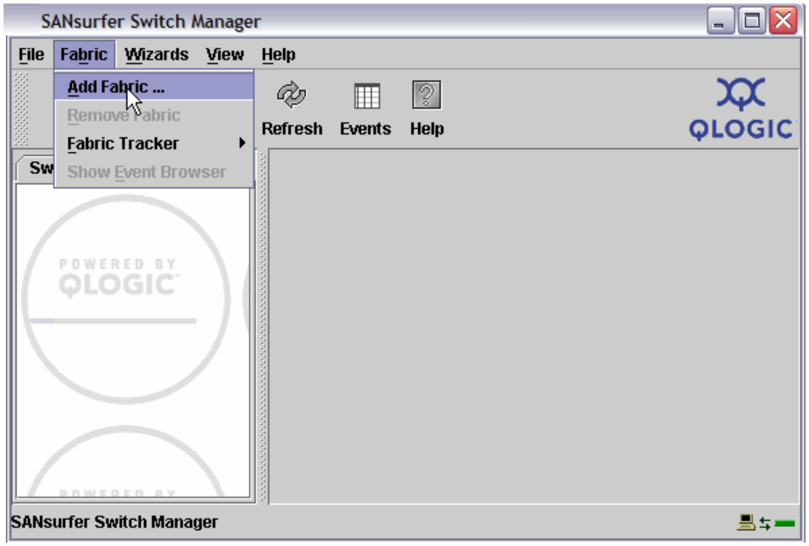
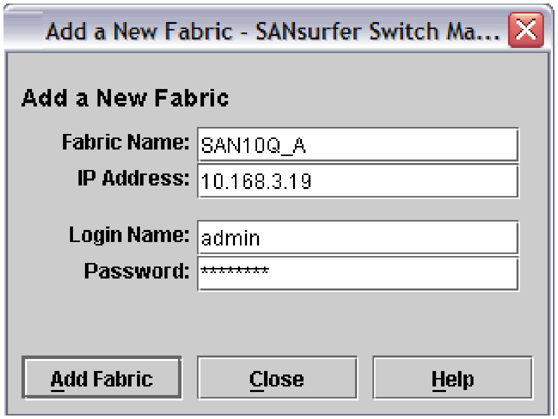

SANsurfer Switch Manager
File
Fabric
Wizards
View
Help
Add Fabric ...
Remove Fabric
Fabric Tracker
Show Event Browser
Refresh
Events
Help
QLOGIC
POWERED BY QLOGIC
SANsurfer Switch Manager

Figure 3-33 SANsurfer Switch Manager Add Fabric

Give your fabric a name, then key in the IP address as well as the admin user name and password, as shown in the example in Figure 3-34. The password is the same one you set in Figure 3-22 on page 668.

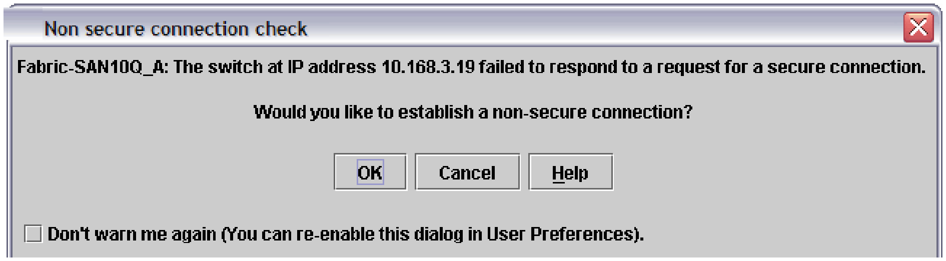

Add a New Fabric - SANsurfer Switch Ma...
Add a New Fabric

Fabric Name: SAN10Q_A
IP Address: 10.168.3.19
Login Name: admin
Password: ********

Add Fabric
Close
Help

Figure 3-34 Add New Fabric

Respond **OK** to the non-secure connection check message shown in Figure 3-35.


Non secure connection check

Fabric-SAN10Q_A: The switch at IP address 10.168.3.19 failed to respond to a request for a secure connection.

Would you like to establish a non-secure connection?

OK
Cancel
Help

☐ Don't warn me again (You can re-enable this dialog in User Preferences).

Figure 3-35 Non secure connection message

You should now get a display similar to Figure 3-36; it shows the status of your switch.

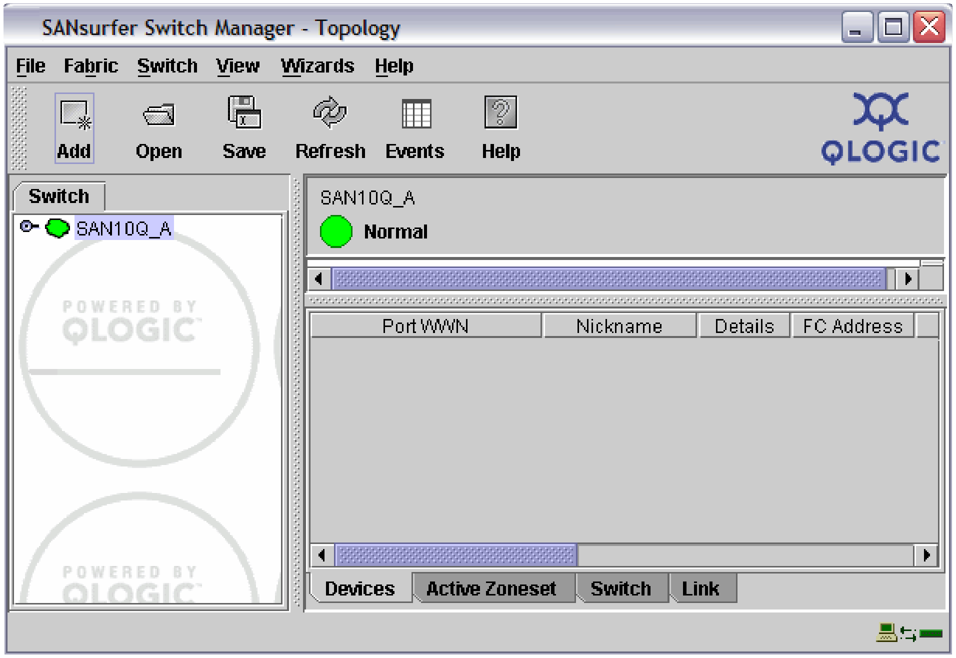

SANsurfer Switch Manager - Topology
File
Fabric
Switch
View
Wizards
Help
Add
Open
Save
Refresh
Events
Help
QLOGIC
Switch
SAN10Q_A
SAN10Q_A
Normal
Port WWN
Nickname
Details
FC Address
Devices
Active Zoneset
Switch
Link

Figure 3-36 New fabric topology

The next step is to exit SANsurfer. Select **File** → **Exit** as shown in Figure 3-37.

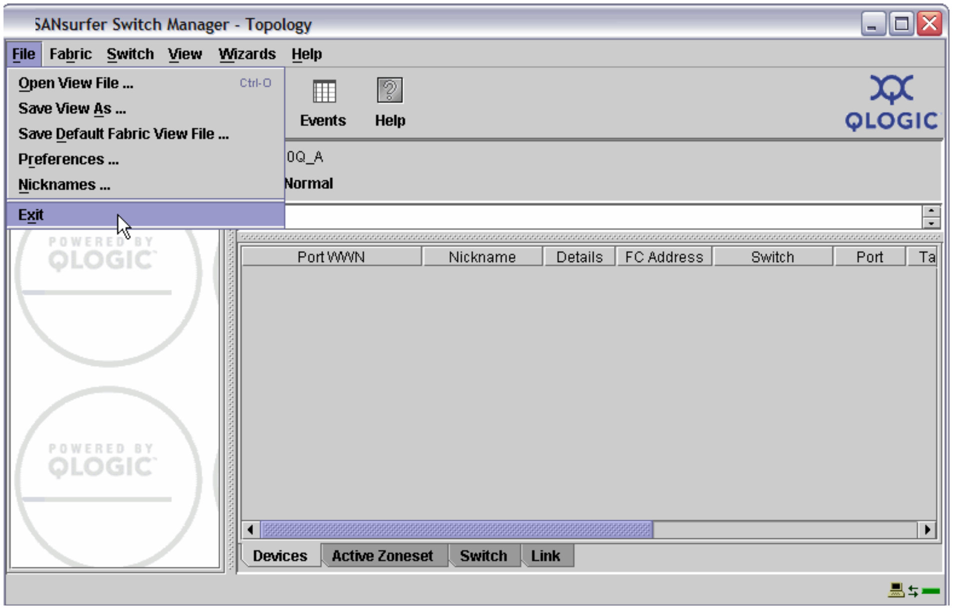
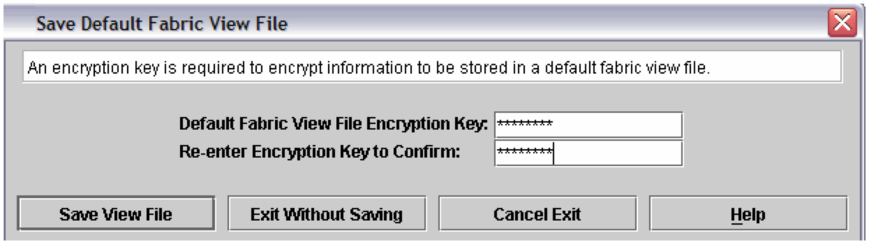

SANsurfer Switch Manager - Topology
File
Fabric
Switch
View
Wizards
Help
Open View File ...
Ctrl-O
Save View As ...
Save Default Fabric View File ...
Preferences ...
Nicknames ...
Exit
Events
Help
QLOGIC
0Q_A
Normal
POWERED BY QLOGIC
Port WWN
Nickname
Details
FC Address
Switch
Port
Ta
Devices
Active Zoneset
Switch
Link

Figure 3-37 Exit SANsurfer

You now get the window shown in Figure 3-38 to enter an encryption key. We recommend that you enter an encryption key to secure your SAN fabric. If this is not done, then anyone who installs SANsurfer can access and modify your fabric, with the default blank key. You can use your switch admin password as the key, or use any other key you can remember.


Save Default Fabric View File
Save View File
Exit Without Saving
Cancel Exit
Help

An encryption key is required to encrypt information to be stored in a default fabric view file.

Default Fabric View File Encryption Key: *********

Re-enter Encryption Key to Confirm: *********

Figure 3-38 Encryption key

This completes the hardware installation process. There is also the possibility to configure the switch from the command line. This procedure is documented in the manual, *System Storage SAN10Q 4 Gbps 10-Port Fibre Channel Switch Type 6918 Installation Guide*. This manual is available on the CD shipped with the switch.

Factory Default Reset

Select the switch you want to reset to default, and from the faceplate menu, select **Switch** → **Restore Factory Defaults,** as shown in Figure 3-39.

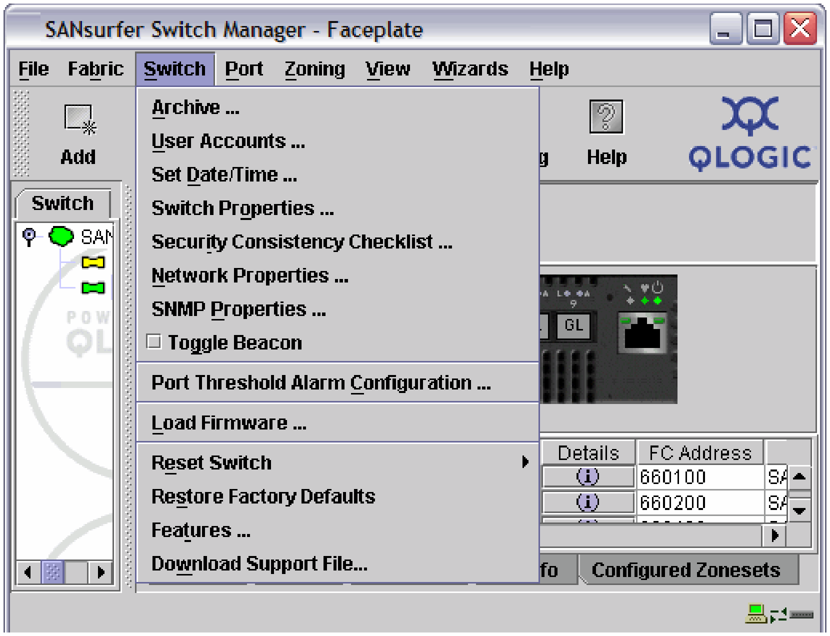
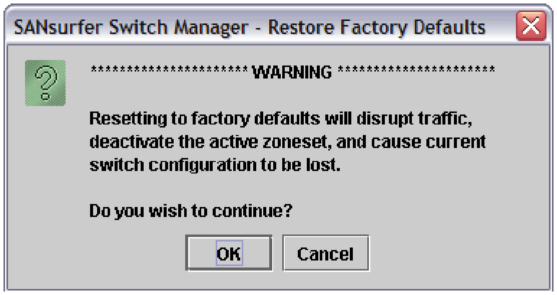

SANsurfer Switch Manager - Faceplate
File
Fabric
Switch
Port
Zoning
View
Wizards
Help
Add
Help
QLOGIC
Switch
Archive ...
User Accounts ...
Set Date/Time ...
Switch Properties ...
Security Consistency Checklist ...
Network Properties ...
SNMP Properties ...
☐ Toggle Beacon
Port Threshold Alarm Configuration ...
Load Firmware ...
Reset Switch
Restore Factory Defaults
Features ...
Download Support File...
Details
FC Address
660100
660200
Configured Zonesets

Figure 3-39 Reset to Factory Defaults

Take note of the warning message, as shown in Figure 3-40, and click **OK** to continue. At this time you lose the connection, because all settings are reset to factory default and you have to start from the beginning to configure the switch.


SANsurfer Switch Manager - Restore Factory Defaults

********************* WARNING *********************

Resetting to factory defaults will disrupt traffic, deactivate the active zoneset, and cause current switch configuration to be lost.

Do you wish to continue?

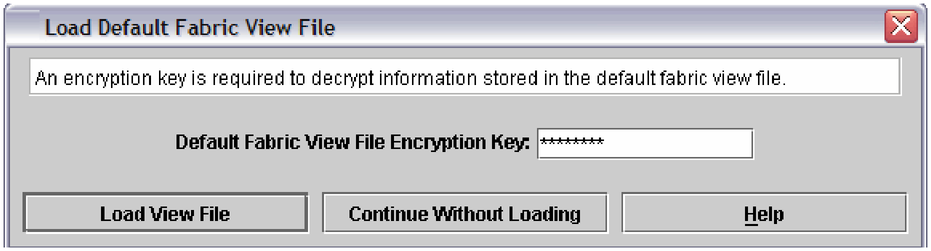
Figure 3-40 Default warning message

Attention: This does not reset the password information to default; to do this, see “Maintenance mode” on page 718.

3.2.4 Configuring the Fibre Channel switch

Prior to installing your devices and ISL link, you have to perform the following procedure.

Start SANsurfer, and enter the key you set during installation, as shown in Figure 3-41.

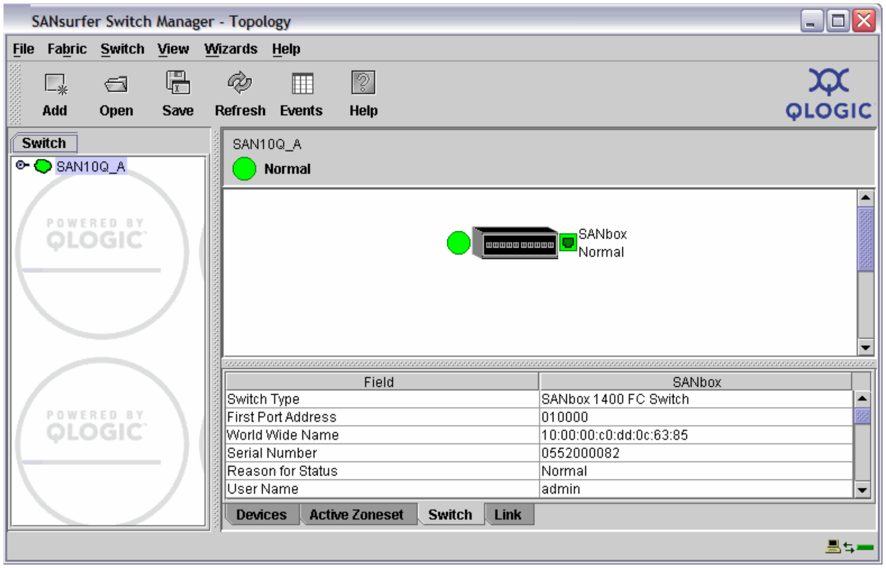

Load Default Fabric View File
Load View File
Continue Without Loading
Help

An encryption key is required to decrypt information stored in the default fabric view file.

Default Fabric View File Encryption Key: ********

Figure 3-41 Enter Encryption Key

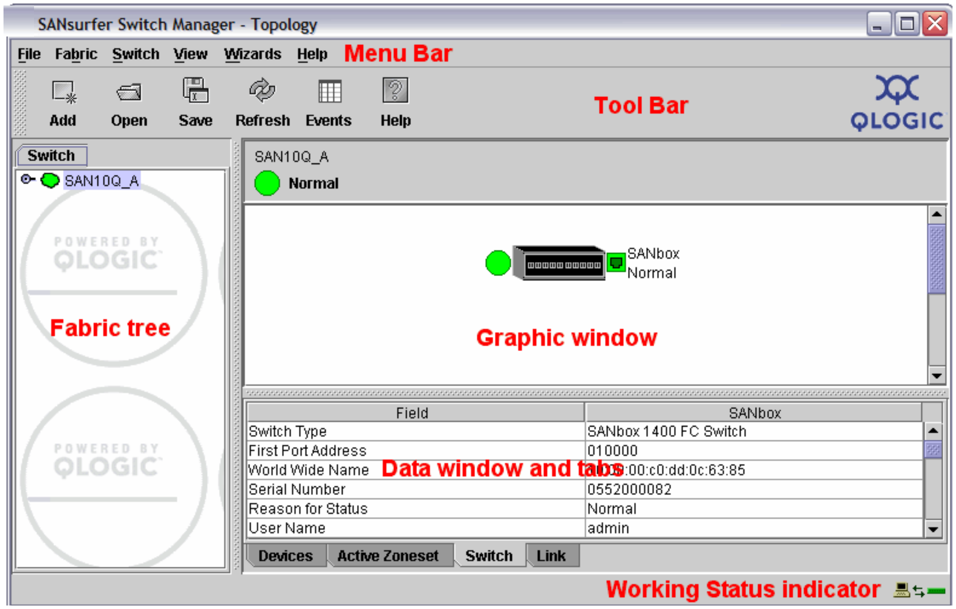
The first window displayed is the Topology display, you can modify the different windows to get a good display as shown in Figure 3-42.


SANsurfer Switch Manager - Topology
File Fabric Switch View Wizards Help
Add
Open
Save
Refresh
Events
Help
QLOGIC
Switch
SAN10Q_A
POWERED BY QLOGIC
SAN10Q_A
Normal
SANbox
Normal
Devices
Active Zoneset
Switch
Link

Field	SANbox
Switch Type	SANbox 1400 FC Switch
First Port Address	010000
World Wide Name	10:00:00:c0:dd:0c:63:85
Serial Number	0552000082
Reason for Status	Normal
User Name	admin

Figure 3-42 SANsurfer Topology window

Figure 3-43 shows the different elements within the SANsurfer main window.


SANsurfer Switch Manager - Topology
File
Fabric
Switch
View
Wizards
Help
Menu Bar
Add
Open
Save
Refresh
Events
Help
Tool Bar
QLOGIC
Switch
SAN10Q_A
POWERED BY QLOGIC
Fabric tree
POWERED BY QLOGIC
SAN10Q_A
Normal
SANbox
Normal
Graphic window
Data window and tabs
Devices
Active Zoneset
Switch
Link
Working Status indicator

Field	SANbox
Switch Type	SANbox 1400 FC Switch
First Port Address	010000
World Wide Name	[illegible]:00:c0:dd:0c:63:85
Serial Number	0552000082
Reason for Status	Normal
User Name	admin

Figure 3-43 SANsurfer Switch Manager

The different elements are:

- Menu Bar
- Toolbar
- Fabric tree
- Graphic window
- Data window and tabs
- Working Status indicator

Using the fabric tree on the left side window, or by double-clicking the switch in the graphic window, you can open the Faceplate window, as shown in Figure 3-44.

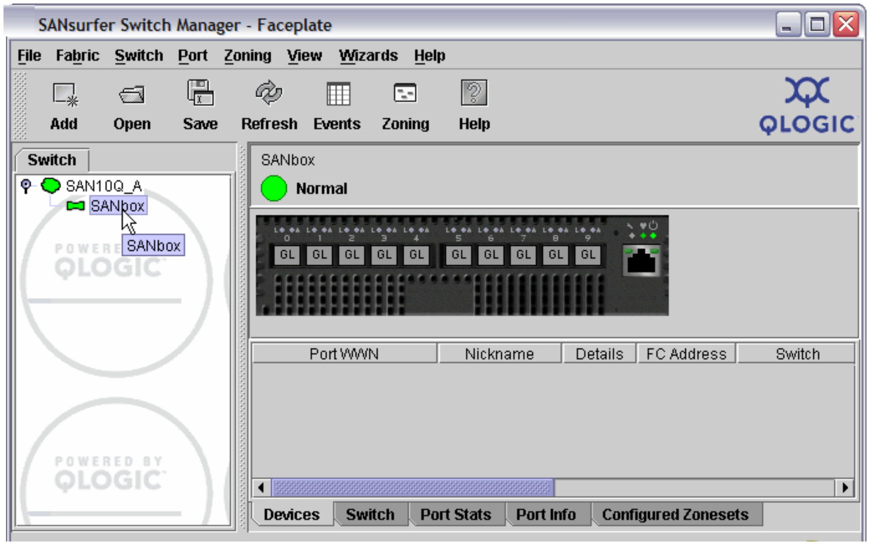

SANsurfer Switch Manager - Faceplate
File Fabric Switch Port Zoning View Wizards Help
Add Open Save Refresh Events Zoning Help
QLOGIC
Switch
SAN10Q_A
SANbox
SANbox
Normal
Port WWN Nickname Details FC Address Switch
Devices Switch Port Stats Port Info Configured Zonesets

Figure 3-44 SANsurfer Faceplate window.

Selecting the **Switch** tab from the Menu Bar, you see all the options to use for configuring the switch, as shown in Figure 3-45.

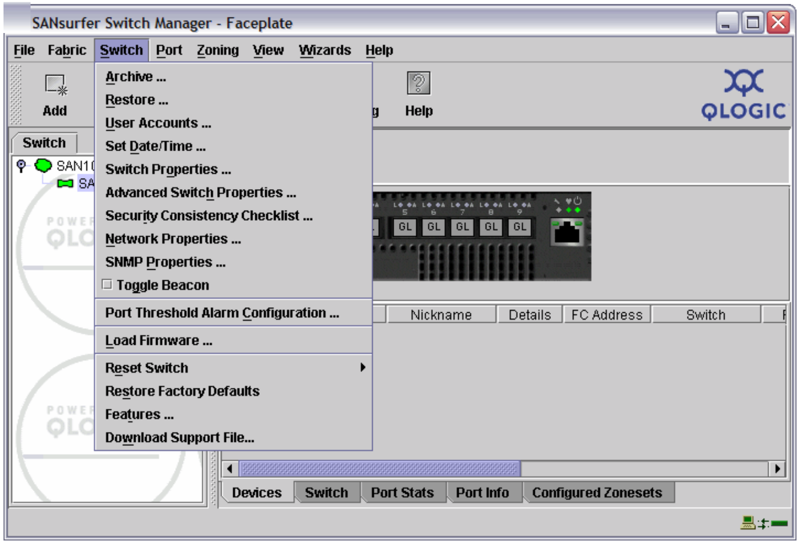
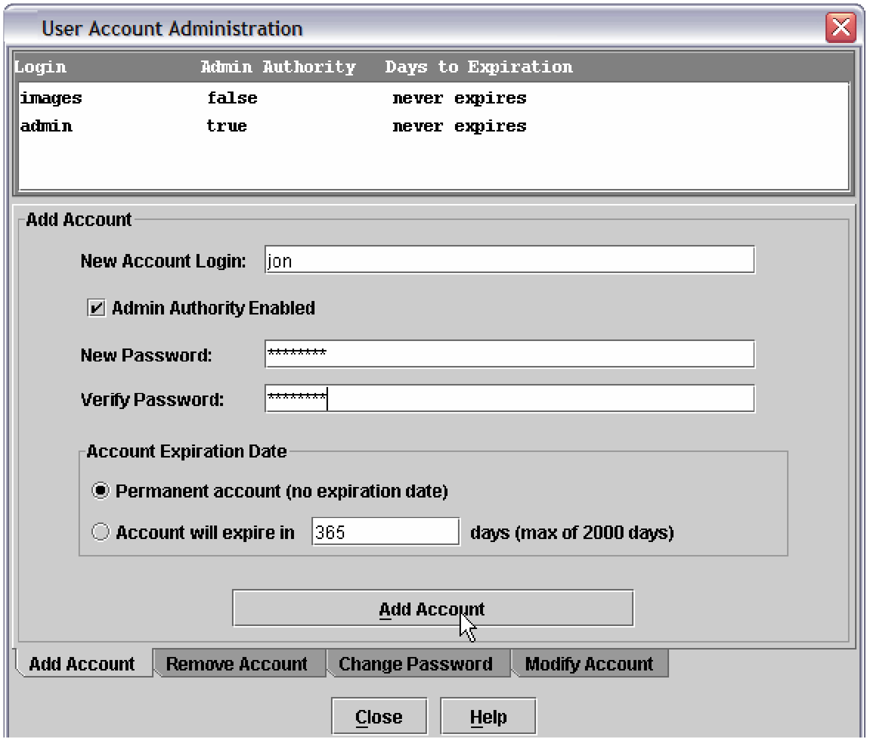

SANsurfer Switch Manager - Faceplate
File Fabric Switch Port Zoning View Wizards Help
Archive ...
Restore ...
User Accounts ...
Set Date/Time ...
Switch Properties ...
Advanced Switch Properties ...
Security Consistency Checklist ...
Network Properties ...
SNMP Properties ...
☐ Toggle Beacon
Port Threshold Alarm Configuration ...
Load Firmware ...
Reset Switch
Restore Factory Defaults
Features ...
Download Support File...
Add Help
QLOGIC
Switch
Nickname Details FC Address Switch
Devices Switch Port Stats Port Info Configured Zonesets

Figure 3-45 SANsurfer switch configuration menu

User Accounts

From the Selecting User Accounts menu, you can add user accounts, as shown in the example in Figure 3-46. Using the bottom tabs, you can also remove, change, and modify any account. The *admin* and *images* accounts cannot be removed.



User Account Administration
Add Account
Account Expiration Date
Add Account
Add Account
Remove Account
Change Password
Modify Account
Close
Help

Login	Admin Authority	Days to Expiration
images	false	never expires
admin	true	never expires

New Account Login: jon

☑ Admin Authority Enabled

New Password: ********

Verify Password: ********

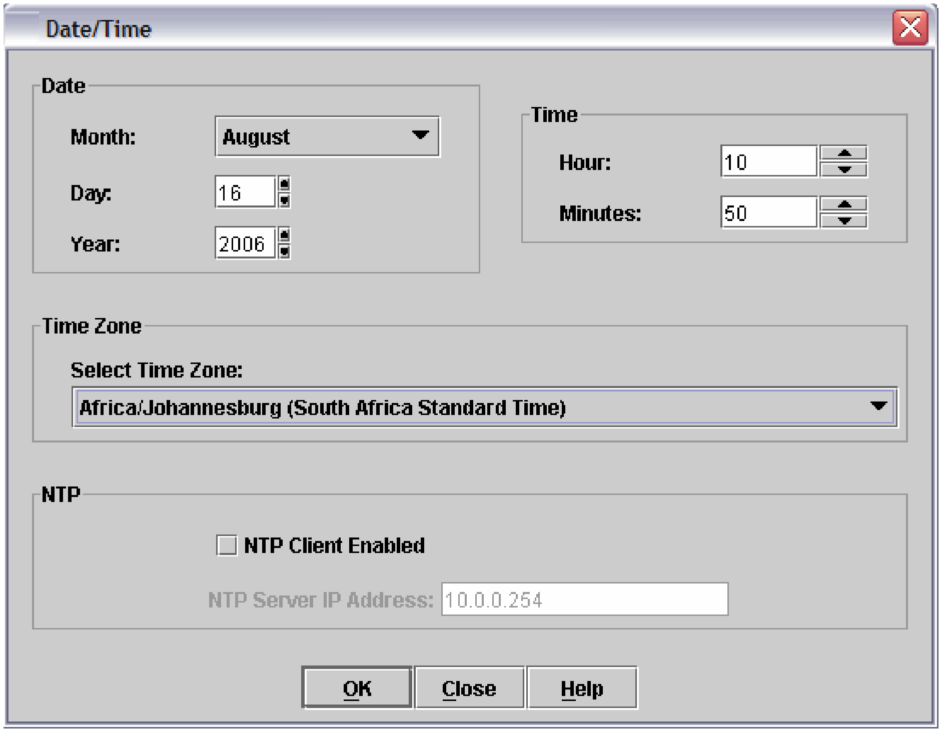
● Permanent account (no expiration date)

○ Account will expire in 365 days (max of 2000 days)

Figure 3-46 User Accounts Administration

Date and Time

Next you can set the date and time of the switch. From this window, shown in Figure 3-47, you can also select your time zone and set up an NTP server.



Date/Time
Date
Time
Time Zone
NTP
OK
Close
Help

Month: August

Day: 16

Year: 2006

Hour: 10

Minutes: 50

Select Time Zone: Africa/Johannesburg (South Africa Standard Time)

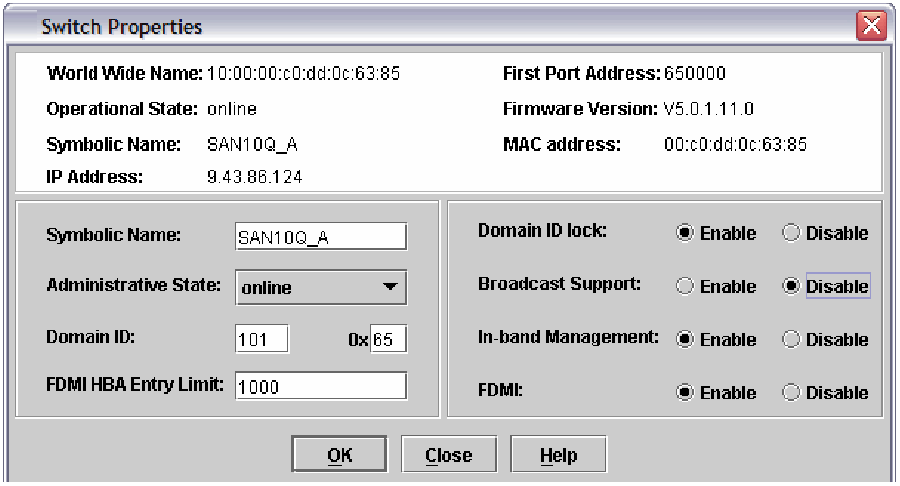
☐ NTP Client Enabled

NTP Server IP Address: 10.0.0.254

Figure 3-47 Date and time setup

Switch Properties

From the menu shown in Figure 3-48, we set all the important switch properties.



World Wide Name: 10:00:00:c0:dd:0c:63:85
First Port Address: 650000
Operational State: online
Firmware Version: V5.0.1.11.0
Symbolic Name: SAN10Q_A
MAC address: 00:c0:dd:0c:63:85
IP Address: 9.43.86.124

Symbolic Name: SAN10Q_A
Administrative State: online
Domain ID: 101 0x 65
FDMI HBA Entry Limit: 1000

Domain ID lock: ● Enable ○ Disable
Broadcast Support: ○ Enable ● Disable
In-band Management: ● Enable ○ Disable
FDMI: ● Enable ○ Disable

Figure 3-48 Switch Properties

The switch properties are:

- **Symbolic Name:** This is the user defined name of the switch, used to easily identify this switch on the management work station, and can be up to 32 characters long.
- **Administrative State:** You can set the switch into 1 of three states.
  - Online
  - Offline
  - Diagnostics
- **Domain ID:** You use this to set your domain ID. The domain ID must be unique for each switch in the fabric.

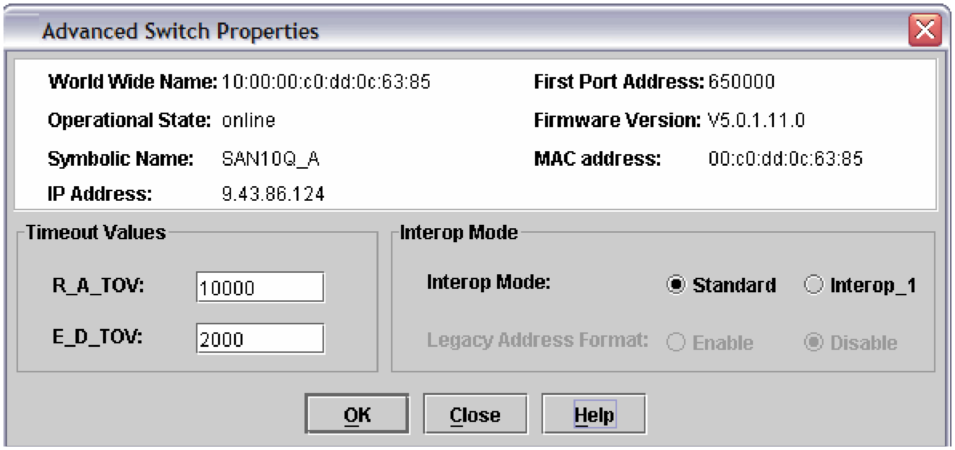
> **Attention:** Make sure that you have done this prior to connecting an ISL to another switch.

- **FDMI HBA Entry Limit:** This sets the limit for the maximum number of HBAs that can be registered with a switch. If the number of HBAs exceeds the maximum number, the FDMI, Fabric Device Management Interface, information, for those HBAs cannot be registered.

- **Domain ID lock:** The default setting is Disabled. This means that the principal switch assigns domain IDs to all joining switches. If you wish to have control over the domain IDs in your fabric, ensure that you enable this button.
- **Broadcast Support:** The default setting is disabled. Broadcast is supported on the switch that allows for TCP/IP support.
- **IN-band Management:** The default setting is enabled. This allows in-band requests to the switch, such as SNMP, Management Server, GUI, and API messaging across Fibre Channel to our switch.
- **FDM:** This enables or disables the Fabric Device Management Interface.

Advanced Switch Properties

You can modify some advanced switch properties from this menu, shown in Figure 3-49.



World Wide Name: 10:00:00:c0:dd:0c:63:85
First Port Address: 650000
Operational State: online
Firmware Version: V5.0.1.11.0
Symbolic Name: SAN10Q_A
MAC address: 00:c0:dd:0c:63:85
IP Address: 9.43.86.124

Timeout Values
R_A_TOV: 10000
E_D_TOV: 2000

Interop Mode
Interop Mode: ● Standard ○ Interop_1
Legacy Address Format: ○ Enable ● Disable

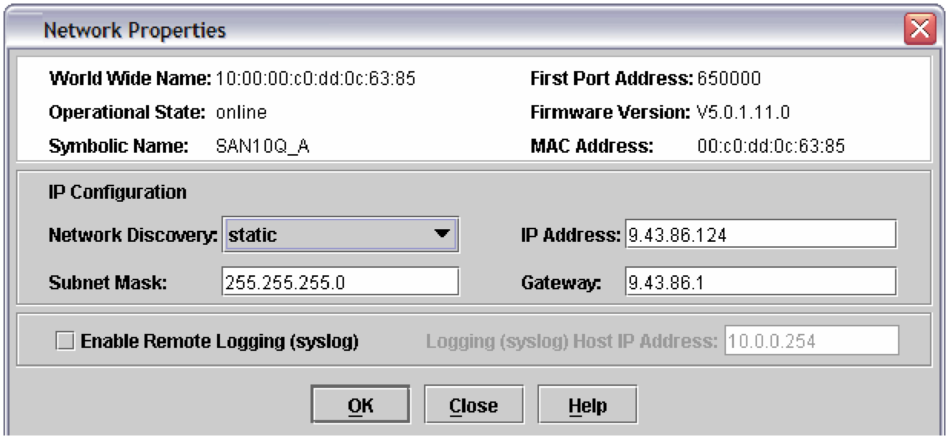
Figure 3-49 Advanced switch properties

These switch properties are:

- **Time-out Values:** We do *not* recommend that you change the default time-out values, because these have to be the same across the fabric.
- **Interop Mode:** Use the *Standard* option for FC-SW-2 compliant switches to propagate only the active zone set to all switches in the fabric. Use the *Interop_1* parameter for non-FC-SW-2 compliant switches to propagate the active zone set and all inactive zone sets to all switches in the fabric.

Network Properties

You can modify your management interface setting from this window, shown in Figure 3-50. You can also set the management interface under the **Network Discovery** option to obtain its IP setting via BootP server, RARP, and DHCP.



World Wide Name: 10:00:00:c0:dd:0c:63:85
Operational State: online
Symbolic Name: SAN10Q_A
First Port Address: 650000
Firmware Version: V5.0.1.11.0
MAC Address: 00:c0:dd:0c:63:85
Network Discovery: static
Subnet Mask: 255.255.255.0
IP Address: 9.43.86.124
Gateway: 9.43.86.1
☐ Enable Remote Logging (syslog)
Logging (syslog) Host IP Address: 10.0.0.254

Figure 3-50 Network Properties.

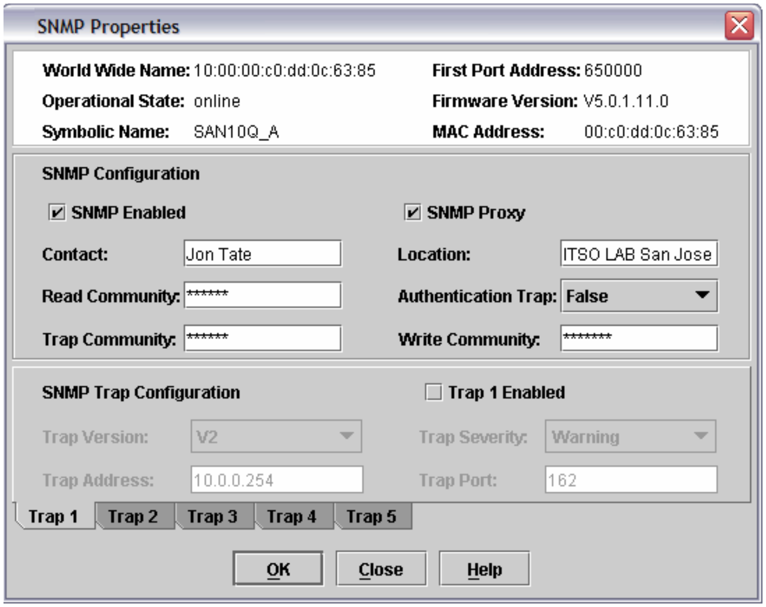
The factory default is set to 10.0.0.1 ant the mask is 255.0.0.0.

When the Enable Remote Logging box is checked, the log entries are sent to the host IP address specified in this field.

> **Attention:** If you change any settings on this window and click **OK**, you could lose connectivity to your switch.

SNMP

Figure 3-51 shows the window where we set up Simple Network Management Protocol. SNMP is the protocol for network management and monitoring of network devices. SNMP security consists of a read community string and a write community string. The read community string *public* and write community string *private* are set at the factory to these well-known defaults and should be changed if SNMP is enabled. SNMP is enabled by default.



World Wide Name: 10:00:00:c0:dd:0c:63:85
First Port Address: 650000
Operational State: online
Firmware Version: V5.0.1.11.0
Symbolic Name: SAN10Q_A
MAC Address: 00:c0:dd:0c:63:85

SNMP Configuration
☑ SNMP Enabled
☑ SNMP Proxy
Contact: Jon Tate
Location: ITSO LAB San Jose
Read Community: ******
Authentication Trap: False
Trap Community: ******
Write Community: *******

SNMP Trap Configuration
☐ Trap 1 Enabled
Trap Version: V2
Trap Severity: Warning
Trap Address: 10.0.0.254
Trap Port: 162

Figure 3-51 SNMP Properties

In the SNMP Configuration area, we can enable or disable SNMP, set our contact and location information, and then set up our community names.

In the SNMP Trap area, we can enable traps, set up the version of SNMP (V1 or V2), severity of traps sent, TCP port number used, and the IP address of our trap receiver. We can set up multiple traps and receivers using the Trap tabs.

3.2.5 Firmware update

In the topics that follow, we show how to obtain the latest firmware and upgrade the switch.

Obtaining the latest firmware

You can obtain the latest firmware as follows:

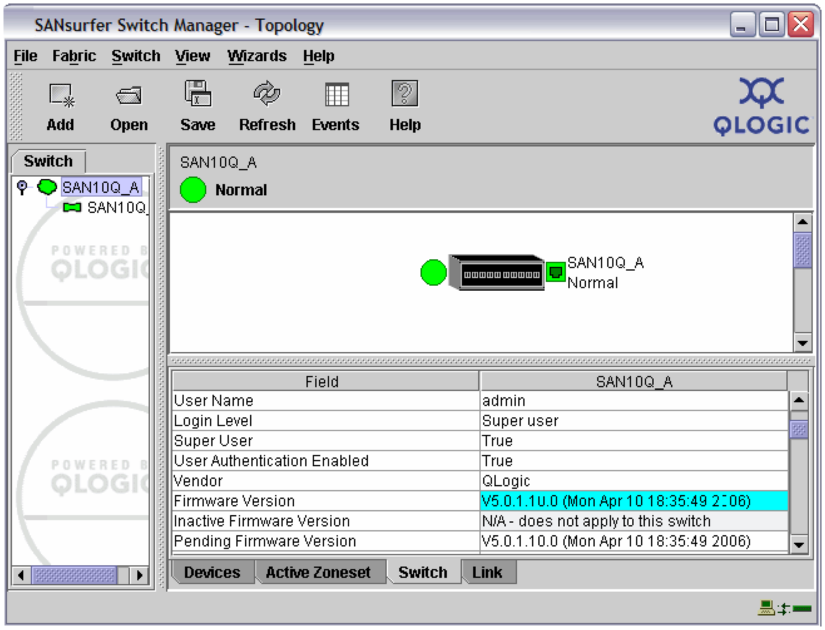
1. Download the latest firmware using the link from the IBM Web site:

   `http://www-03.ibm.com/servers/storage/support/san/san10q/downloading.html`

2. This links you to the QLogic Web site dedicated to IBM, from which you can download both the latest firmware and SANsurfer.
3. Download the firmware onto your management workstation.

Upgrading the switch

From the SANsurfer Topology window, we can see the current version of our switch, as shown in Figure 3-52.

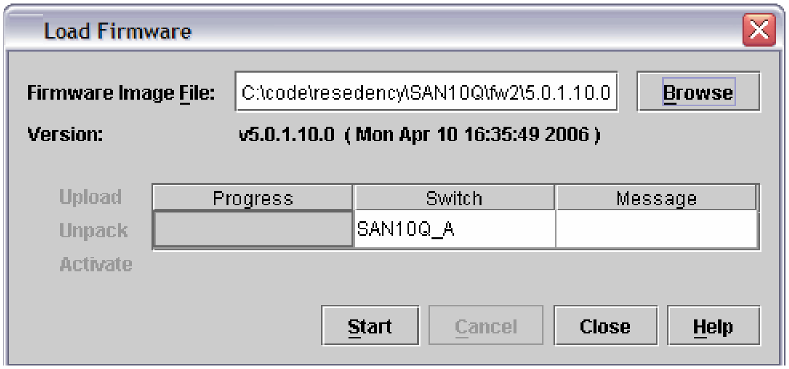

SANsurfer Switch Manager - Topology
File Fabric Switch View Wizards Help
Add Open Save Refresh Events Help
QLOGIC
Switch
SAN10Q_A
SAN10Q_
SAN10Q_A
Normal
SAN10Q_A
Normal
Devices Active Zoneset Switch Link

Field	SAN10Q_A
User Name	admin
Login Level	Super user
Super User	True
User Authentication Enabled	True
Vendor	QLogic
Firmware Version	V5.0.1.10.0 (Mon Apr 10 18:35:49 2006)
Inactive Firmware Version	N/A - does not apply to this switch
Pending Firmware Version	V5.0.1.10.0 (Mon Apr 10 18:35:49 2006)

Figure 3-52 Check switch firmware level

Select the switch you wish to upgrade in the fabric tree and then select **Switch** → **Load Firmware**.

The Load Firmware frame is now displayed, as shown in Figure 3-53. Select the **Browse** button.


Load Firmware
Browse
Upload
Unpack
Activate
Start
Cancel
Close
Help

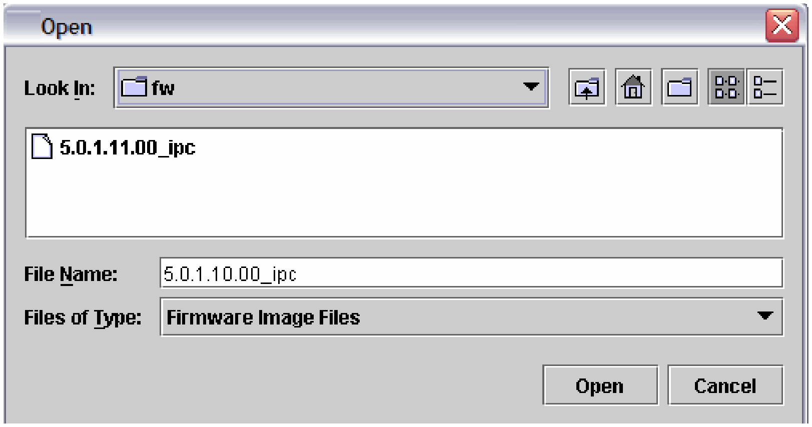
Firmware Image File: C:\code\resedency\SAN10Q\fw2\5.0.1.10.0

Version: v5.0.1.10.0 (Mon Apr 10 16:35:49 2006)

Progress	Switch	Message
	SAN10Q_A	

Figure 3-53 Load Firmware

Using the **Look In** button, shown in Figure 3-54, browse to the directory into which you downloaded the firmware. Select the correct firmware image and click the **Open** button.


Open
Open
Cancel

Look In: fw

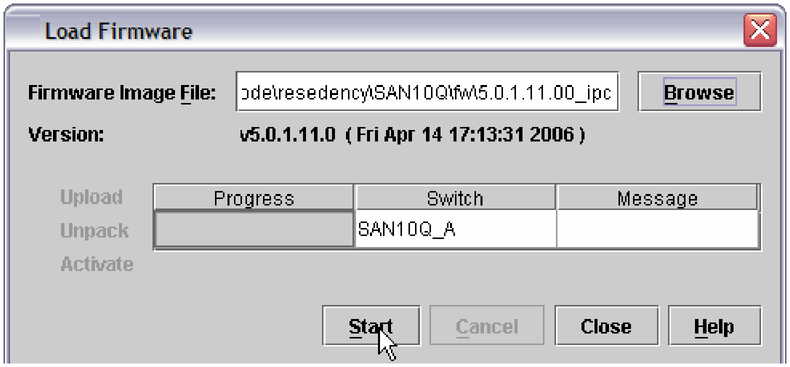
5.0.1.11.00_ipc

File Name: 5.0.1.10.00_ipc

Files of Type: Firmware Image Files

Figure 3-54 Open file

On the Load Firmware window, you now see the version you selected displayed in the version field, shown in Figure 3-55. Click the **Start** button to begin the download.


Load Firmware
Browse
Upload
Unpack
Activate
Start
Cancel
Close
Help

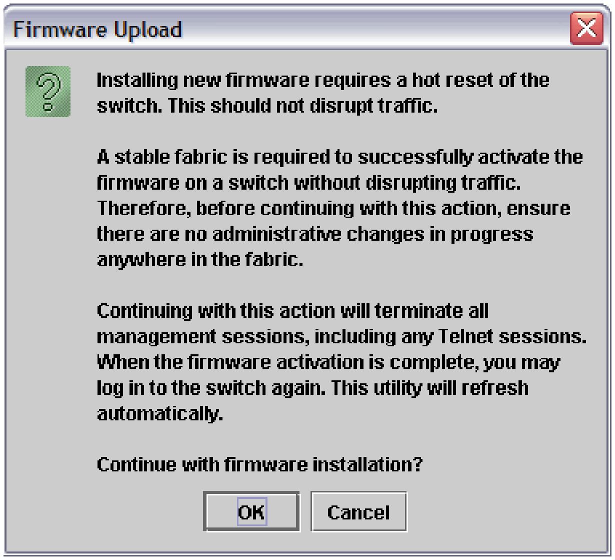
Firmware Image File: ode\resedency\SAN10Q\fw\5.0.1.11.00_ipc

Version: v5.0.1.11.0 (Fri Apr 14 17:13:31 2006)

Progress	Switch	Message
	SAN10Q_A	

Figure 3-55 Load Firmware start

You now receive a warning message as shown in Figure 3-56. Read the message and then click **OK** to continue.



Installing new firmware requires a hot reset of the switch. This should not disrupt traffic.

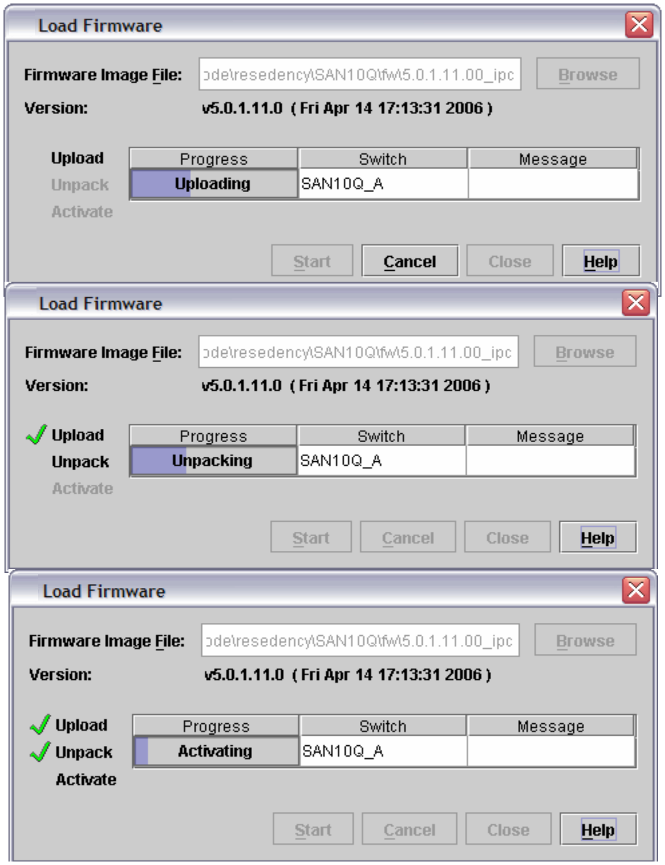
A stable fabric is required to successfully activate the firmware on a switch without disrupting traffic. Therefore, before continuing with this action, ensure there are no administrative changes in progress anywhere in the fabric.

Continuing with this action will terminate all management sessions, including any Telnet sessions. When the firmware activation is complete, you may log in to the switch again. This utility will refresh automatically.

Continue with firmware installation?

Figure 3-56 Warning message

The window shown in Figure 3-57 displays the progress of the activation process.



Firmware Image File: ɔde\resedency\SAN10Q\fw\5.0.1.11.00_ipc

Version: v5.0.1.11.0 (Fri Apr 14 17:13:31 2006)

Progress	Switch	Message
Uploading	SAN10Q_A	

Firmware Image File: ɔde\resedency\SAN10Q\fw\5.0.1.11.00_ipc

Version: v5.0.1.11.0 (Fri Apr 14 17:13:31 2006)

Progress	Switch	Message
Unpacking	SAN10Q_A	

Firmware Image File: ɔde\resedency\SAN10Q\fw\5.0.1.11.00_ipc

Version: v5.0.1.11.0 (Fri Apr 14 17:13:31 2006)

Progress	Switch	Message
Activating	SAN10Q_A	

Figure 3-57 Activation progress windows.

During the final phase, the switch performs a hot reset. Fabric services are unavailable for a short period (30-75 seconds); this is shown in Figure 3-58.

> **Note:** To ensure that a Non-Disruptive Code Load and Activation operation is successful, do not attempt to do any administrative changes to the fabric during a firmware update. If a changes to the fabric are attempted during this process, this might disrupt the firmware activation process.

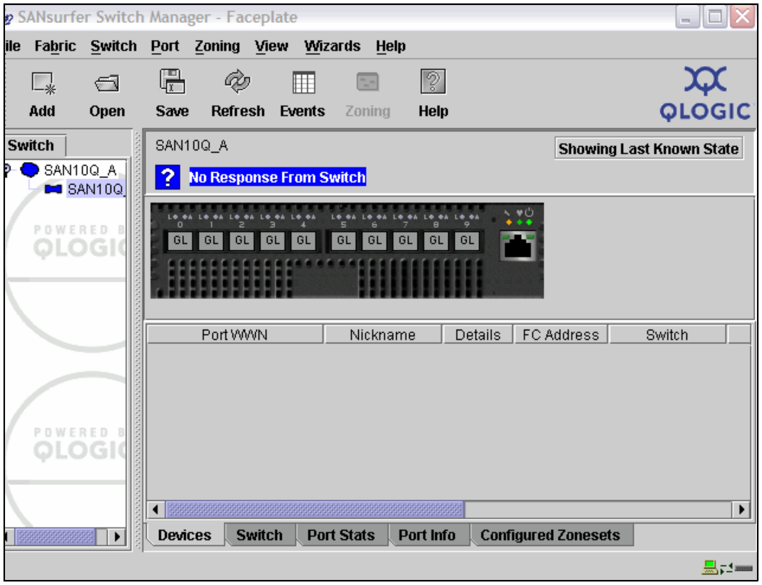
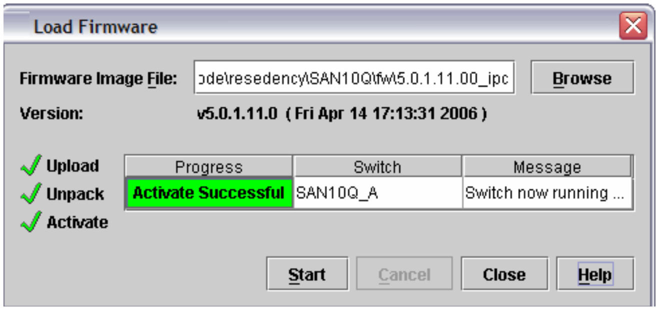

SANsurfer Switch Manager - Faceplate
ile Fabric Switch Port Zoning View Wizards Help
Add Open Save Refresh Events Zoning Help
QLOGIC
Switch
SAN10Q_A
SAN10Q_
POWERED B
QLOGIC
SAN10Q_A
Showing Last Known State
No Response From Switch
Port WWN
Nickname
Details
FC Address
Switch
Devices Switch Port Stats Port Info Configured Zonesets

Figure 3-58 Hot reset of switch

Finally, you get the Activation Successful message, shown in Figure 3-59. Click the **Close** button to exit.


Load Firmware
Browse
Start Cancel Close Help

Firmware Image File: ɔde\resedency\SAN10Q\fw\5.0.1.11.00_ipc

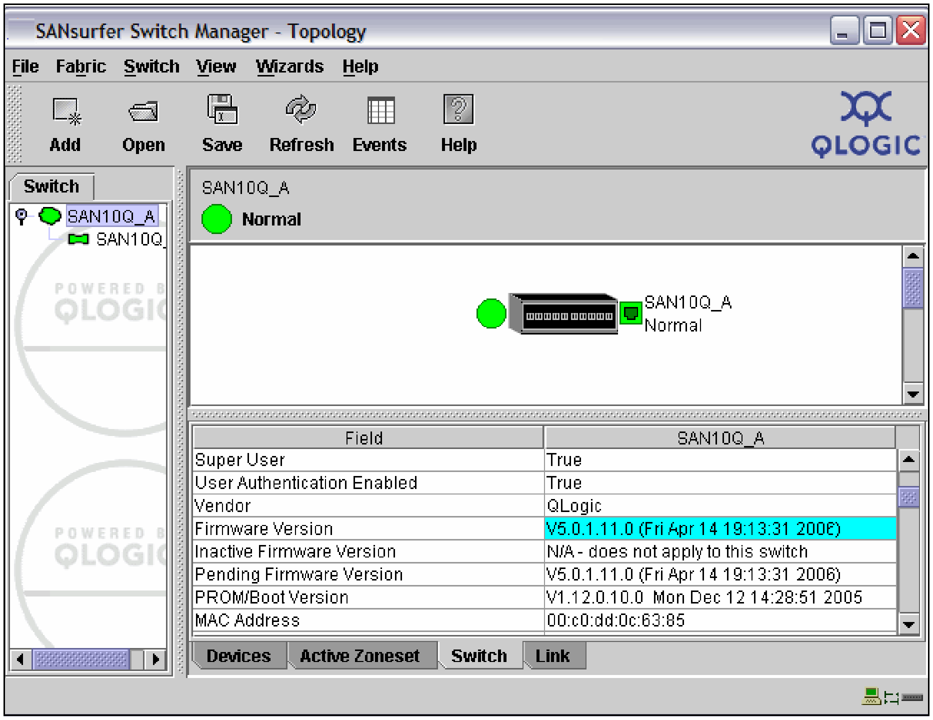
Version: v5.0.1.11.0 (Fri Apr 14 17:13:31 2006)

✓ Upload
✓ Unpack
✓ Activate

Progress	Switch	Message
Activate Successful	SAN10Q_A	Switch now running ...

Figure 3-59 Activation successful

When the Firmware upgrade is completed, you can check your active level of the switch from the Topology display as shown in Figure 3-60.


SANsurfer Switch Manager - Topology
File
Fabric
Switch
View
Wizards
Help
Add
Open
Save
Refresh
Events
Help
QLOGIC
Switch
SAN10Q_A
SAN10Q_
SAN10Q_A
Normal
SAN10Q_A
Normal
Devices
Active Zoneset
Switch
Link

Field	SAN10Q_A
Super User	True
User Authentication Enabled	True
Vendor	QLogic
Firmware Version	V5.0.1.11.0 (Fri Apr 14 19:13:31 2006)
Inactive Firmware Version	N/A - does not apply to this switch
Pending Firmware Version	V5.0.1.11.0 (Fri Apr 14 19:13:31 2006)
PROM/Boot Version	V1.12.0.10.0 Mon Dec 12 14:28:51 2005
MAC Address	00:c0:dd:0c:63:85

Figure 3-60 Firmware versions

3.2.6 Zoning

In the topics that follow we discuss zoning.

Zoning limits

These are the zoning limits for the QLogic:

- The maximum number of zone sets is 256.
- The maximum number of zones is 2000.
- The maximum number of aliases is 2500.
- The maximum number of total zone and alias members is 10,000.
- The maximum number of zone linkages to zonesets is 2000. Every time a zone is added to a zoneset, this constitutes a linkage.
- The maximum number of zone members is 2000. Aliases are considered zone members when added to a zone.
- The maximum number of zone members that can be added to any alias is 2000.

Zone types

The SAN10Q supports hard zoning and soft zoning.

Hard zoning is, as its name suggests, enforced by the hardware, Hard zoning membership can be defined only by domain ID and port number, and supports all port types.

Soft zoning, as its name suggests, is enforced by the name server. Soft zoning membership can be defined by Fibre Channel address, domain ID and port number, world wide name, or a combination. Soft zoning supports all port types.

With reference to Figure 3-61, we utilize two SAN10Q switches to create a redundant SAN.

The first step would be to install and configure both switches using the previous topics in this book. We have linked both switches together utilizing an ISL link and have plugged all devices into the switches.

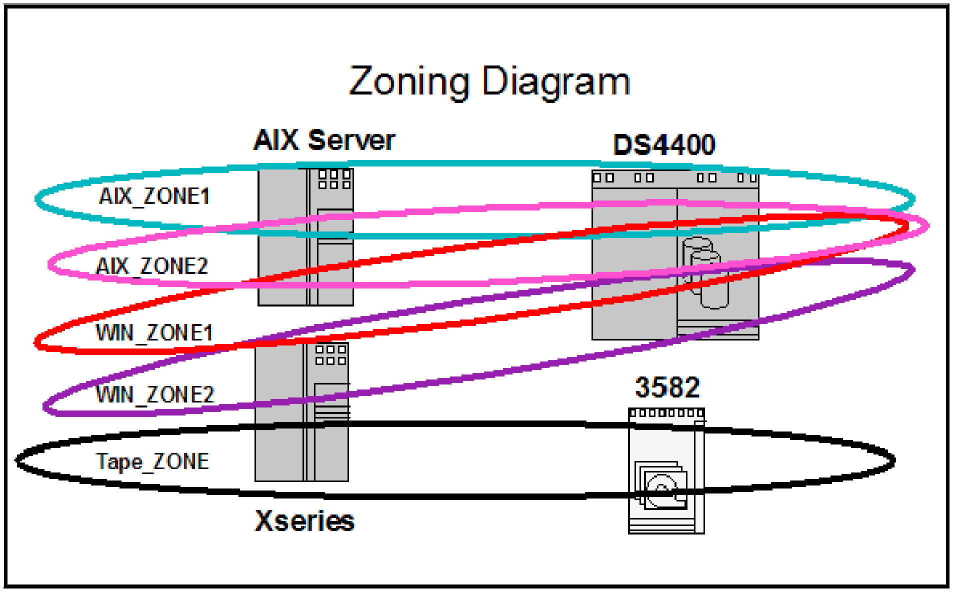
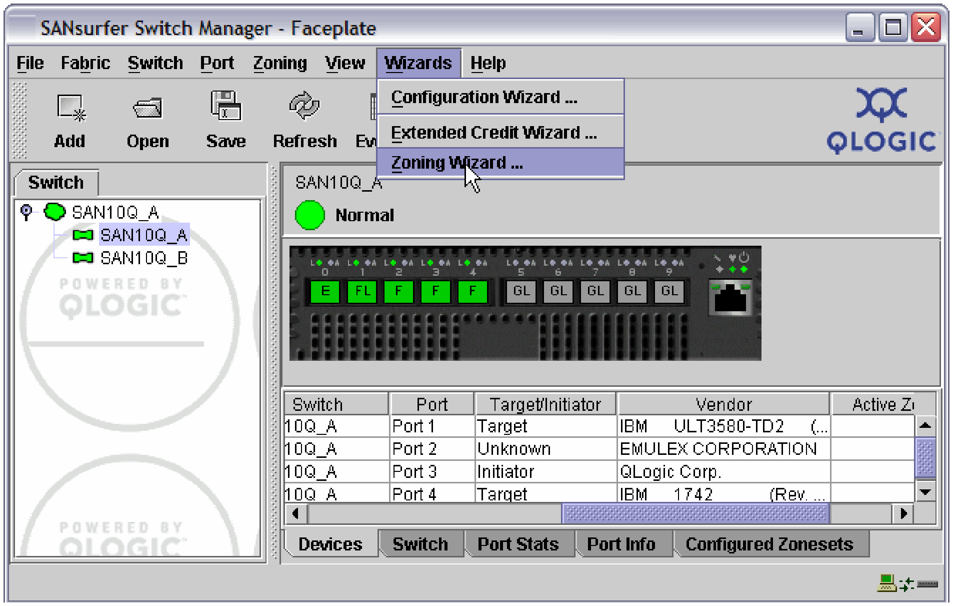

Zoning Diagram
AIX Server
DS4400
AIX_ZONE1
AIX_ZONE2
WIN_ZONE1
WIN_ZONE2
3582
Tape_ZONE
Xseries

Figure 3-61 Zoning diagram

Zoning Wizard

For small, simple installations, you can use the Zoning Wizard, which brings up a series of dialogs windows that leads you through the process of zoning a fabric. To open the Zoning Wizard, select **Wizards** → **Zoning Wizard.** The wizard is only supported on windows servers and is self explanatory as shown in Figure 3-62.

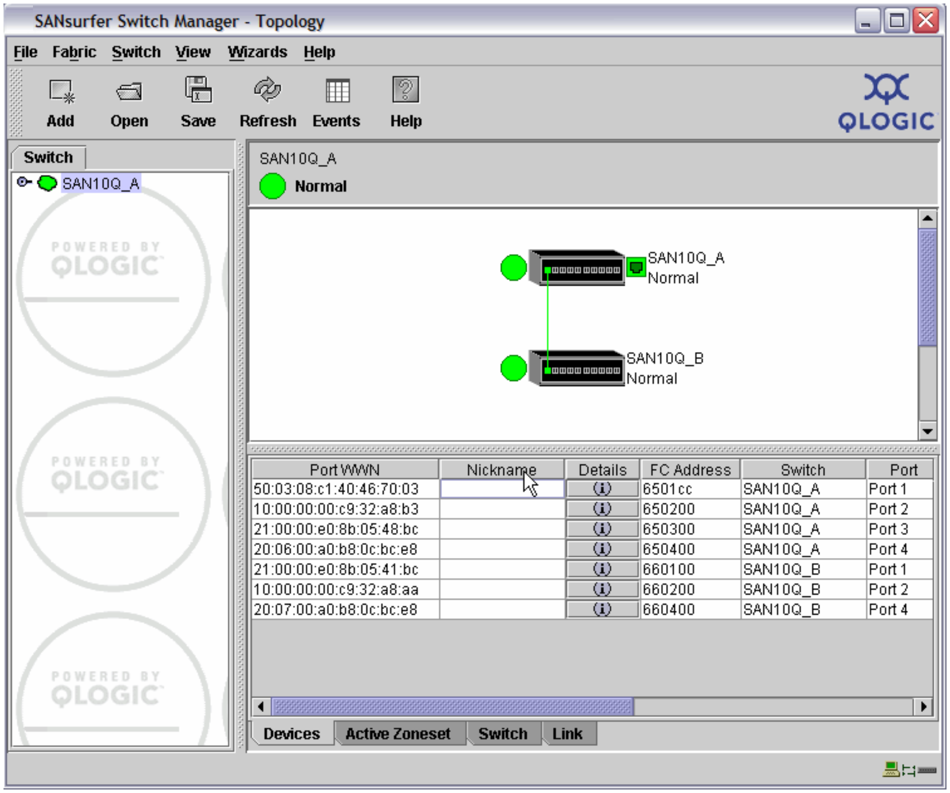

SANsurfer Switch Manager - Faceplate
File
Fabric
Switch
Port
Zoning
View
Wizards
Help
Configuration Wizard ...
Extended Credit Wizard ...
Zoning Wizard ...
Add
Open
Save
Refresh
Ev
QLOGIC
Switch
SAN10Q_A
SAN10Q_A
SAN10Q_B
POWERED BY QLOGIC
SAN10Q_A
Normal
E
FL
F
F
F
GL
GL
GL
GL
GL
Devices
Switch
Port Stats
Port Info
Configured Zonesets

Switch	Port	Target/Initiator	Vendor	Active Z
10Q_A	Port 1	Target	IBM ULT3580-TD2 (...	
10Q_A	Port 2	Unknown	EMULEX CORPORATION	
10Q_A	Port 3	Initiator	QLogic Corp.	
10Q_A	Port 4	Target	IBM 1742 (Rev. ...	

Figure 3-62 Zoning Wizard

Zoning startup

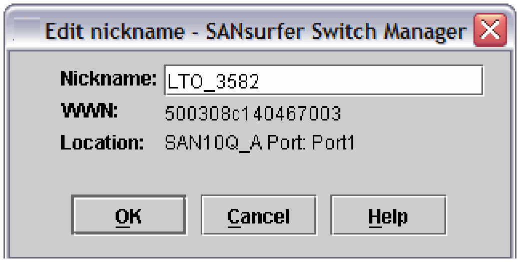
To make zoning easier, we can give each WWN a nickname, and to do this, we double-click the nickname field in the devices menu shown in Figure 3-63. This is not compulsory, but it can make it less complicated to manage the SAN.


SANsurfer Switch Manager - Topology
File
Fabric
Switch
View
Wizards
Help
Add
Open
Save
Refresh
Events
Help
QLOGIC
Switch
SAN10Q_A
SAN10Q_A
Normal
SAN10Q_A
Normal
SAN10Q_B
Normal
Devices
Active Zoneset
Switch
Link

Port WWN	Nickname	Details	FC Address	Switch	Port
50:03:08:c1:40:46:70:03		ⓘ	6501cc	SAN10Q_A	Port 1
10:00:00:00:c9:32:a8:b3		ⓘ	650200	SAN10Q_A	Port 2
21:00:00:e0:8b:05:48:bc		ⓘ	650300	SAN10Q_A	Port 3
20:06:00:a0:b8:0c:bc:e8		ⓘ	650400	SAN10Q_A	Port 4
21:00:00:e0:8b:05:41:bc		ⓘ	660100	SAN10Q_B	Port 1
10:00:00:00:c9:32:a8:aa		ⓘ	660200	SAN10Q_B	Port 2
20:07:00:a0:b8:0c:bc:e8		ⓘ	660400	SAN10Q_B	Port 4

Figure 3-63 Topology display

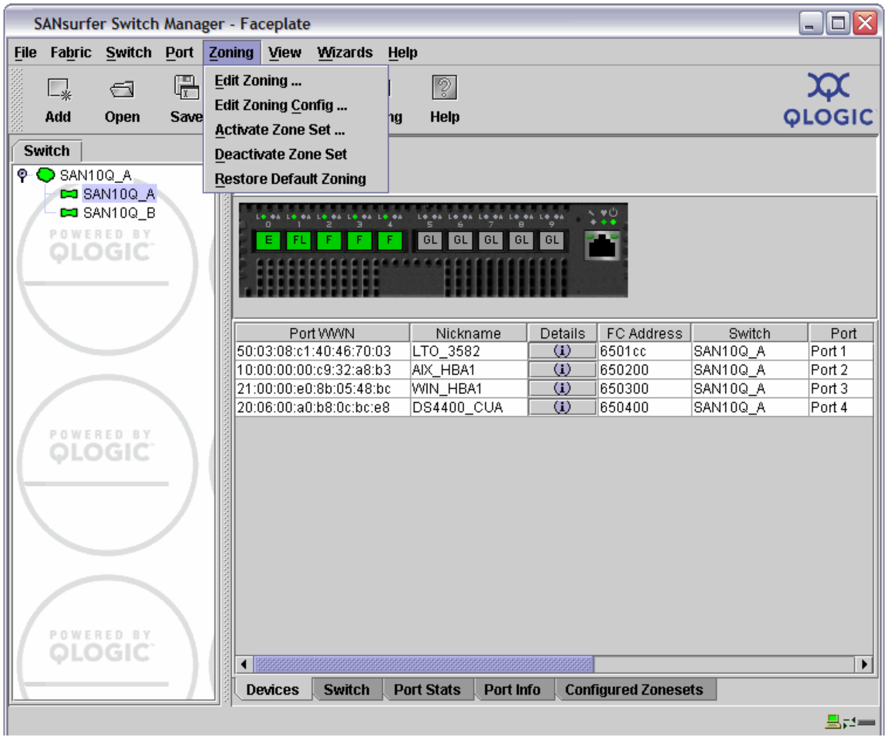
We now give each of the attached WWNs a nickname, as shown in Figure 3-64.


Edit nickname - SANsurfer Switch Manager
OK
Cancel
Help

Nickname: LTO_3582
WWN: 500308c140467003
Location: SAN10Q_A Port: Port1

Figure 3-64 Adding nickname

From the Faceplate window of any switch, we select **Zoning** → **Edit Zoning** as shown in Figure 3-65.


SANsurfer Switch Manager - Faceplate
File
Fabric
Switch
Port
Zoning
View
Wizards
Help
Edit Zoning ...
Edit Zoning Config ...
Activate Zone Set ...
Deactivate Zone Set
Restore Default Zoning
Add
Open
Save
ng
Help
QLOGIC
Switch
SAN10Q_A
SAN10Q_A
SAN10Q_B
POWERED BY QLOGIC
E
FL
F
F
F
GL
GL
GL
GL
GL
Devices
Switch
Port Stats
Port Info
Configured Zonesets

Port WWN	Nickname	Details	FC Address	Switch	Port
50:03:08:c1:40:46:70:03	LTO_3582	ⓘ	6501cc	SAN10Q_A	Port 1
10:00:00:00:c9:32:a8:b3	AIX_HBA1	ⓘ	650200	SAN10Q_A	Port 2
21:00:00:e0:8b:05:48:bc	WIN_HBA1	ⓘ	650300	SAN10Q_A	Port 3
20:06:00:a0:b8:0c:bc:e8	DS4400_CUA	ⓘ	650400	SAN10Q_A	Port 4

Figure 3-65 Starting Zoning configuration

The *Edit Zoning* window is now displayed, as shown in Figure 3-66. You notice the nicknames that were set up previously are displayed in the *Members* window. If you do not set up nicknames, then you see the WWN of each device.

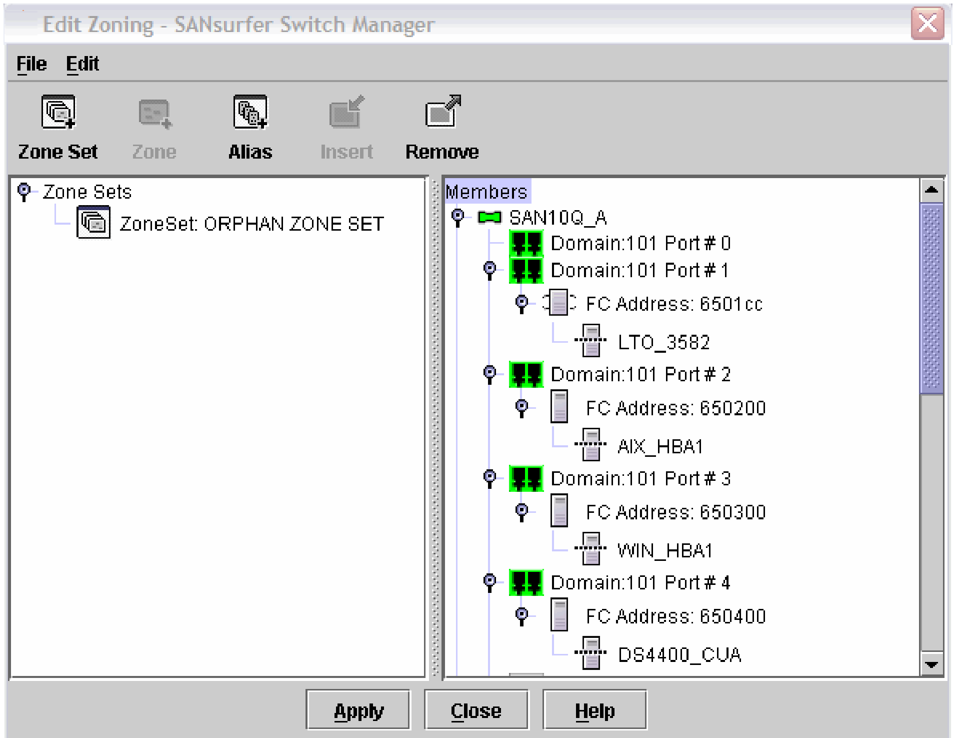
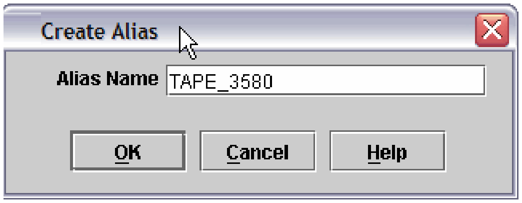

Edit Zoning - SANsurfer Switch Manager
File
Edit
Zone Set
Zone
Alias
Insert
Remove
Zone Sets
ZoneSet: ORPHAN ZONE SET
Members
SAN10Q_A
Domain:101 Port # 0
Domain:101 Port # 1
FC Address: 6501cc
LTO_3582
Domain:101 Port # 2
FC Address: 650200
AIX_HBA1
Domain:101 Port # 3
FC Address: 650300
WIN_HBA1
Domain:101 Port # 4
FC Address: 650400
DS4400_CUA
Apply
Close
Help

Figure 3-66 Edit Zoning window

Creating an alias

An alias is a named set of ports or devices that are grouped together for convenience. You can add an alias to one or more zones. However, you cannot add a zone to an alias, nor can an alias be a member of another alias. To create an alias, from the window shown in Figure 3-66, select the **Alias** button.

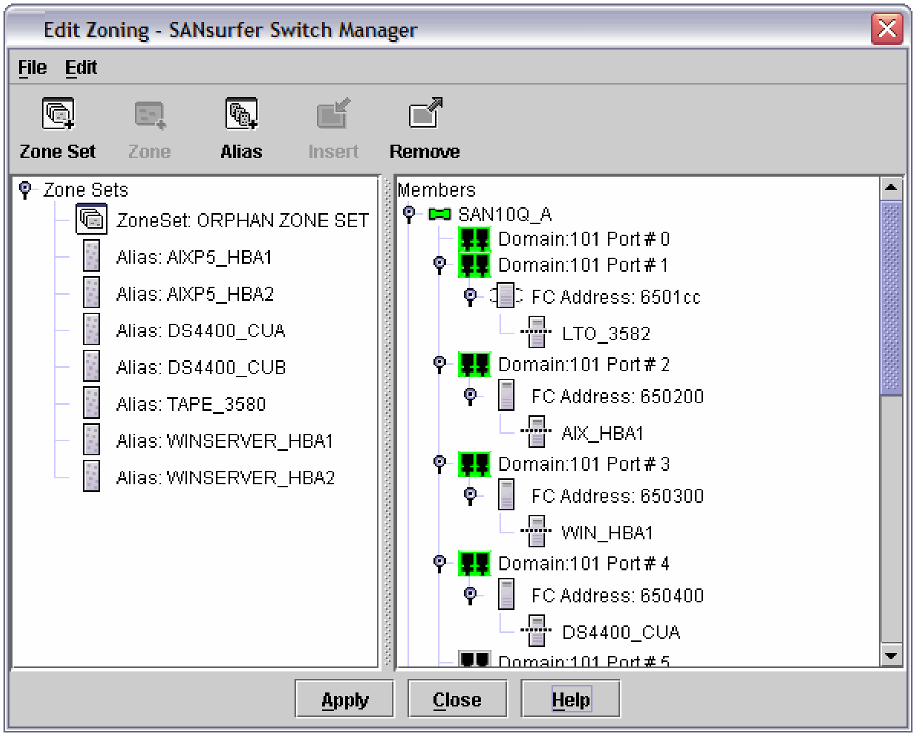
Enter the alias name in the window shown in Figure 3-67, and repeat this step for all the alias names you wish to create.


Create Alias
OK
Cancel
Help

Alias Name: TAPE_3580

Figure 3-67 Create Alias

When this is done, you have a list under Zone Sets of all the alias names you have defined, as shown in Figure 3-68.



Zone Sets
ZoneSet: ORPHAN ZONE SET
Alias: AIXP5_HBA1
Alias: AIXP5_HBA2
Alias: DS4400_CUA
Alias: DS4400_CUB
Alias: TAPE_3580
Alias: WINSERVER_HBA1
Alias: WINSERVER_HBA2

Members
SAN10Q_A
Domain:101 Port # 0
Domain:101 Port # 1
FC Address: 6501cc
LTO_3582
Domain:101 Port # 2
FC Address: 650200
AIX_HBA1
Domain:101 Port # 3
FC Address: 650300
WIN_HBA1
Domain:101 Port # 4
FC Address: 650400
DS4400_CUA
Domain:101 Port # 5

Figure 3-68 Alias names

There are three methods you can use to add members to an alias:

- To use the drag-and-drop method, click and hold down the mouse button on the member to be added to the alias. Drag the selected member from the right pane to the alias in the left pane.
- Select the alias in the left pane and the member to add to that alias in the right pane, and then **Edit** → **Add Members**.
- Select the alias in the left pane, select the member to add to that alias in the right pane, and click the **Insert** button.

Using one of these methods, add the members to the alias names as shown in Figure 3-69.

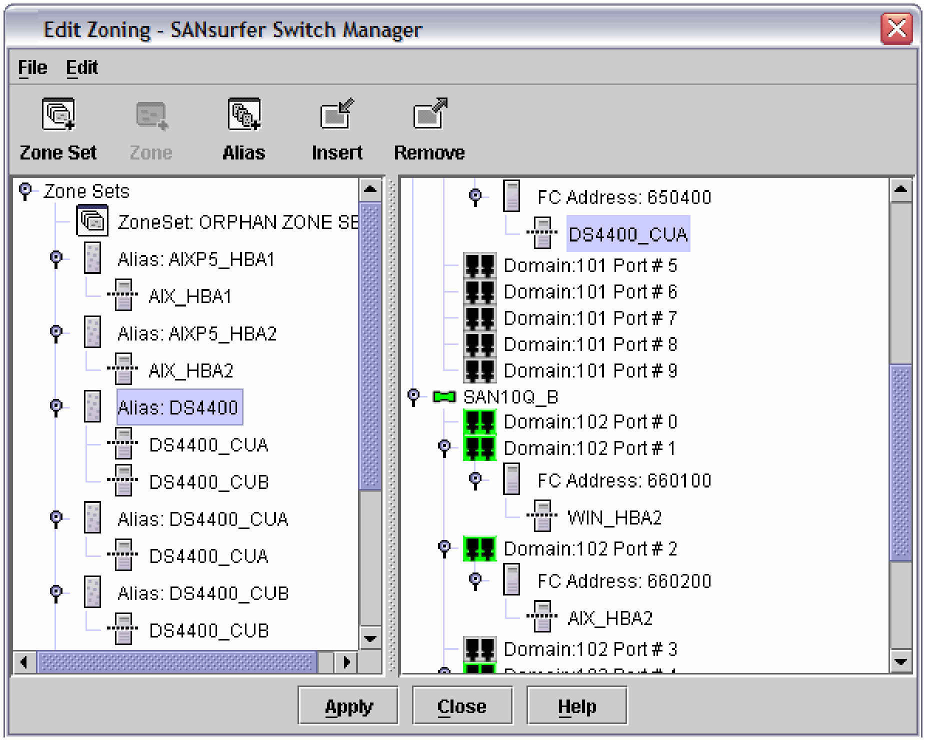
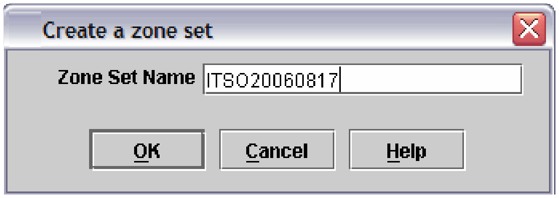

Edit Zoning - SANsurfer Switch Manager
File
Edit
Zone Set
Zone
Alias
Insert
Remove
Zone Sets
ZoneSet: ORPHAN ZONE SE
Alias: AIXP5_HBA1
AIX_HBA1
Alias: AIXP5_HBA2
AIX_HBA2
Alias: DS4400
DS4400_CUA
DS4400_CUB
Alias: DS4400_CUA
DS4400_CUA
Alias: DS4400_CUB
DS4400_CUB
FC Address: 650400
DS4400_CUA
Domain:101 Port # 5
Domain:101 Port # 6
Domain:101 Port # 7
Domain:101 Port # 8
Domain:101 Port # 9
SAN10Q_B
Domain:102 Port # 0
Domain:102 Port # 1
FC Address: 660100
WIN_HBA2
Domain:102 Port # 2
FC Address: 660200
AIX_HBA2
Domain:102 Port # 3
Apply
Close
Help

Figure 3-69 Adding a Member to an Alias

Creating a zone set and zones

By clicking the **Zone Set** icon as shown in Figure 3-69, you get a window to enter the zoneset name as shown in Figure 3-70. Enter your zoneset name and click **OK**.


Create a zone set
OK
Cancel
Help

Zone Set Name ITSO20060817

Figure 3-70 Create Zoneset

Now click the zoneset you have just created and click the **Zone** button as shown in Figure 3-71.

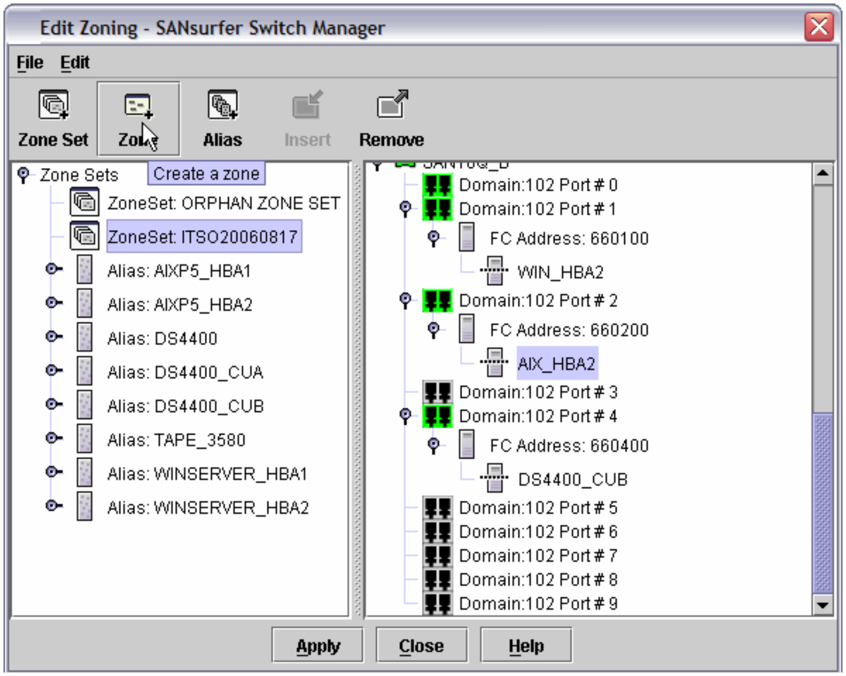
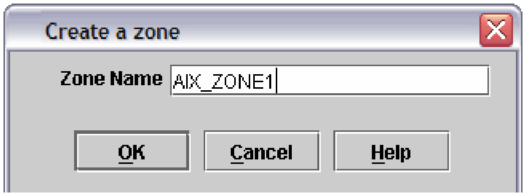

Edit Zoning - SANsurfer Switch Manager
File Edit
Zone Set
Zone
Alias
Insert
Remove
Zone Sets
Create a zone
ZoneSet: ORPHAN ZONE SET
ZoneSet: ITSO20060817
Alias: AIXP5_HBA1
Alias: AIXP5_HBA2
Alias: DS4400
Alias: DS4400_CUA
Alias: DS4400_CUB
Alias: TAPE_3580
Alias: WINSERVER_HBA1
Alias: WINSERVER_HBA2
Domain:102 Port # 0
Domain:102 Port # 1
FC Address: 660100
WIN_HBA2
Domain:102 Port # 2
FC Address: 660200
AIX_HBA2
Domain:102 Port # 3
Domain:102 Port # 4
FC Address: 660400
DS4400_CUB
Domain:102 Port # 5
Domain:102 Port # 6
Domain:102 Port # 7
Domain:102 Port # 8
Domain:102 Port # 9
Apply
Close
Help

Figure 3-71 Zone set created

Enter the name of the zone you wish to create as shown in Figure 3-72, and repeat this step for all the zones you wish to create.


Create a zone
OK
Cancel
Help

Zone Name: AIX_ZONE1

Figure 3-72 Create zone

Under the zoneset you created, you see all the zone names you have just created, as shown in Figure 3-73.

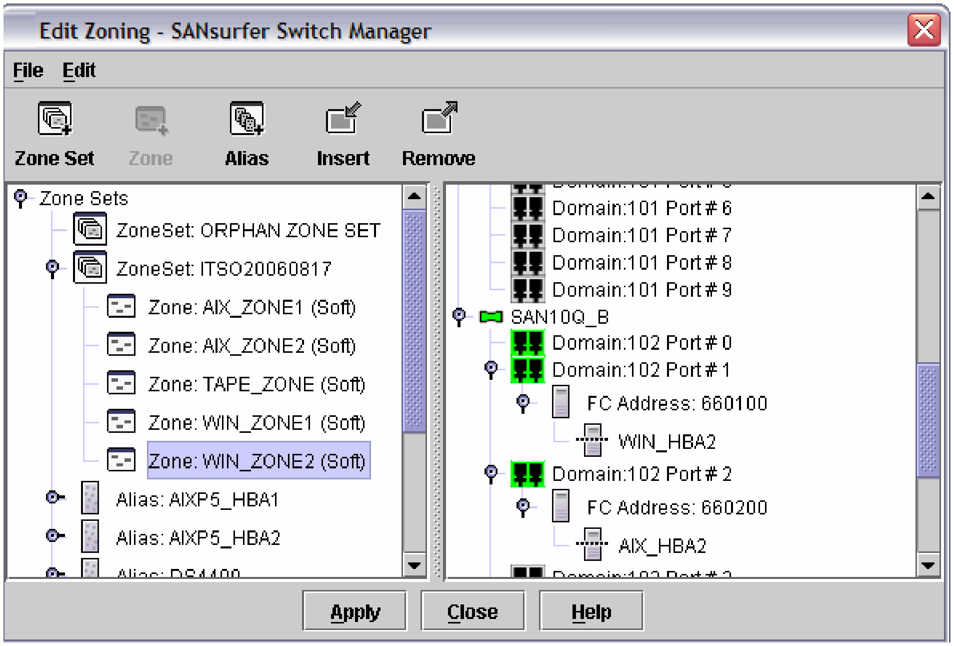

Edit Zoning - SANsurfer Switch Manager
File
Edit
Zone Set
Zone
Alias
Insert
Remove
Zone Sets
ZoneSet: ORPHAN ZONE SET
ZoneSet: ITSO20060817
Zone: AIX_ZONE1 (Soft)
Zone: AIX_ZONE2 (Soft)
Zone: TAPE_ZONE (Soft)
Zone: WIN_ZONE1 (Soft)
Zone: WIN_ZONE2 (Soft)
Alias: AIXP5_HBA1
Alias: AIXP5_HBA2
Domain:101 Port # 6
Domain:101 Port # 7
Domain:101 Port # 8
Domain:101 Port # 9
SAN10Q_B
Domain:102 Port # 0
Domain:102 Port # 1
FC Address: 660100
WIN_HBA2
Domain:102 Port # 2
FC Address: 660200
AIX_HBA2
Apply
Close
Help

Figure 3-73 Zones created

By default, all zones are set up for soft zoning. To change any details of the zone you have created, such as zone type and name, right-click the zone and select the action from the menu options displayed, as shown in Figure 3-74.

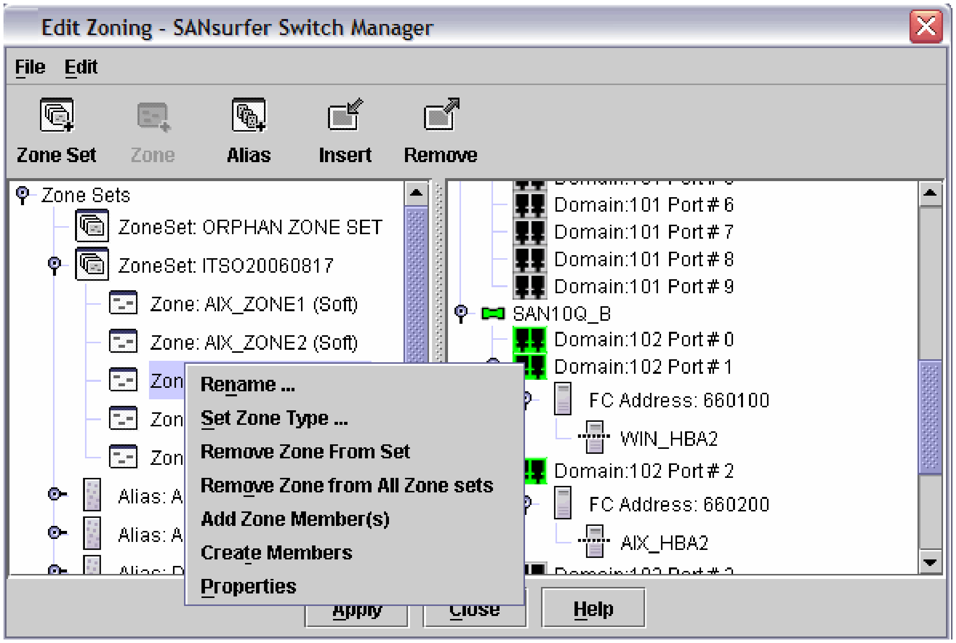

Edit Zoning - SANsurfer Switch Manager
File
Edit
Zone Set
Zone
Alias
Insert
Remove
Zone Sets
ZoneSet: ORPHAN ZONE SET
ZoneSet: ITSO20060817
Zone: AIX_ZONE1 (Soft)
Zone: AIX_ZONE2 (Soft)
Zon
Zon
Zon
Alias: A
Alias: A
Domain:101 Port # 6
Domain:101 Port # 7
Domain:101 Port # 8
Domain:101 Port # 9
SAN10Q_B
Domain:102 Port # 0
Domain:102 Port # 1
FC Address: 660100
WIN_HBA2
Domain:102 Port # 2
FC Address: 660200
AIX_HBA2
Rename ...
Set Zone Type ...
Remove Zone From Set
Remove Zone from All Zone sets
Add Zone Member(s)
Create Members
Properties
Apply
Close
Help

Figure 3-74 Zone Modification

Adding members to a zone can be done in a number of ways:

- Select a member by alias name, and drag it into the zone.
- Select one or more members by port number, Fibre Channel address, or World Wide Name in the device tree. Then select the zone in which to add members, and select the **Insert** button, as shown in Figure 3-75.
- Select a member by port number, Fibre Channel address, or World Wide Name in the device tree, and drag it into the zone. You can select and drag multiple ports or devices by pressing and holding the Control key while dragging into the required zone.

Do this to configure all your zones and click the **Apply** button to save changes to the zoning database.

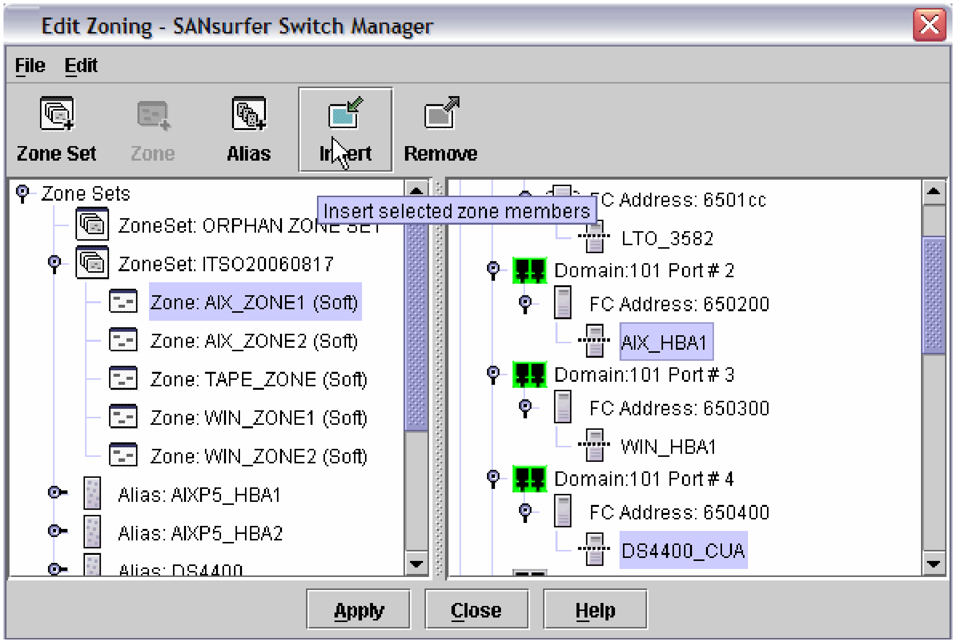
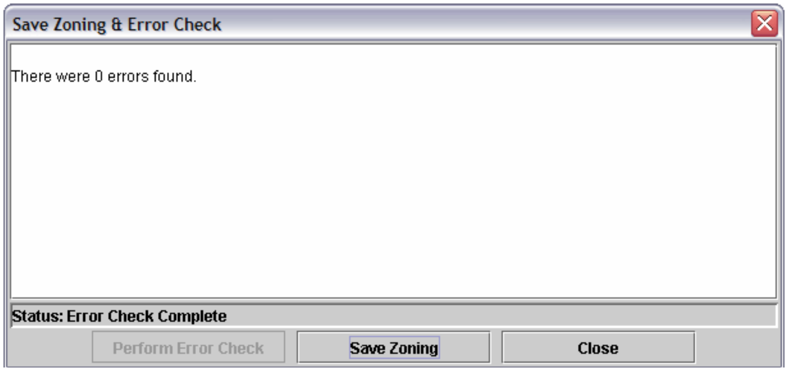

Edit Zoning - SANsurfer Switch Manager
File
Edit
Zone Set
Zone
Alias
Insert
Remove
Insert selected zone members
Zone Sets
ZoneSet: ORPHAN ZONE SET
ZoneSet: ITSO20060817
Zone: AIX_ZONE1 (Soft)
Zone: AIX_ZONE2 (Soft)
Zone: TAPE_ZONE (Soft)
Zone: WIN_ZONE1 (Soft)
Zone: WIN_ZONE2 (Soft)
Alias: AIXP5_HBA1
Alias: AIXP5_HBA2
Alias: DS4400
FC Address: 6501cc
LTO_3582
Domain:101 Port # 2
FC Address: 650200
AIX_HBA1
Domain:101 Port # 3
FC Address: 650300
WIN_HBA1
Domain:101 Port # 4
FC Address: 650400
DS4400_CUA
Apply
Close
Help

Figure 3-75 Adding zone members

Click the **Save Zoning** button, from the window shown in Figure 3-76.

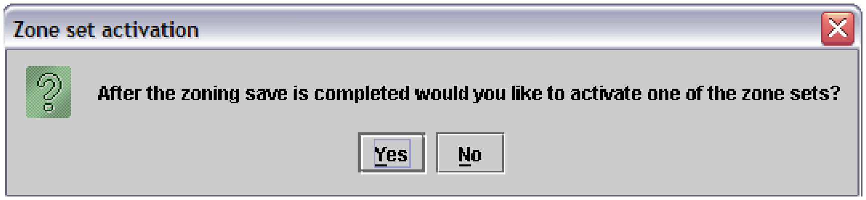

Save Zoning & Error Check
Perform Error Check
Save Zoning
Close

There were 0 errors found.

Status: Error Check Complete

Figure 3-76 Save Zoning

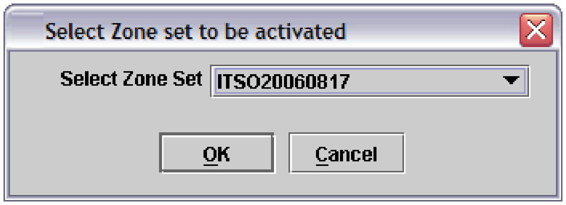
Click **Yes** to activate, from the window shown in Figure 3-77.


Zone set activation
Yes
No

After the zoning save is completed would you like to activate one of the zone sets?

Figure 3-77 Zone set activation

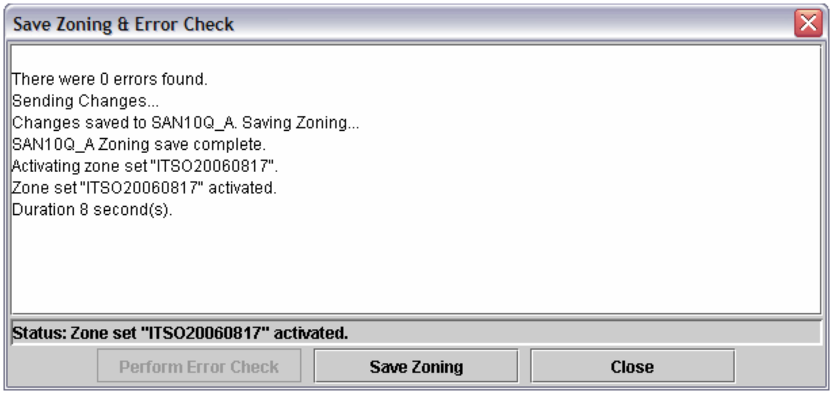
Select the zone set you wish to activate and click **OK**, from the window shown in Figure 3-78.


Select Zone set to be activated
OK
Cancel

Select Zone Set: ITSO20060817

Figure 3-78 Zones set to be activated

Check the status line of the window shown in Figure 3-79 to see if the zoneset was activated.


Save Zoning & Error Check
Perform Error Check
Save Zoning
Close

```
There were 0 errors found.
Sending Changes...
Changes saved to SAN10Q_A. Saving Zoning...
SAN10Q_A Zoning save complete.
Activating zone set "ITSO20060817".
Zone set "ITSO20060817" activated.
Duration 8 second(s).
```

Status: Zone set "ITSO20060817" activated.

Figure 3-79 Zoneset activation complete

Modifying Zoning

Using the Edit Zoning window, as shown in Figure 3-80. you can add, delete, and modify all zoning information. You can create a new zone set using the previous steps and create new zones into this new zone set. You can also modify the active zone set.

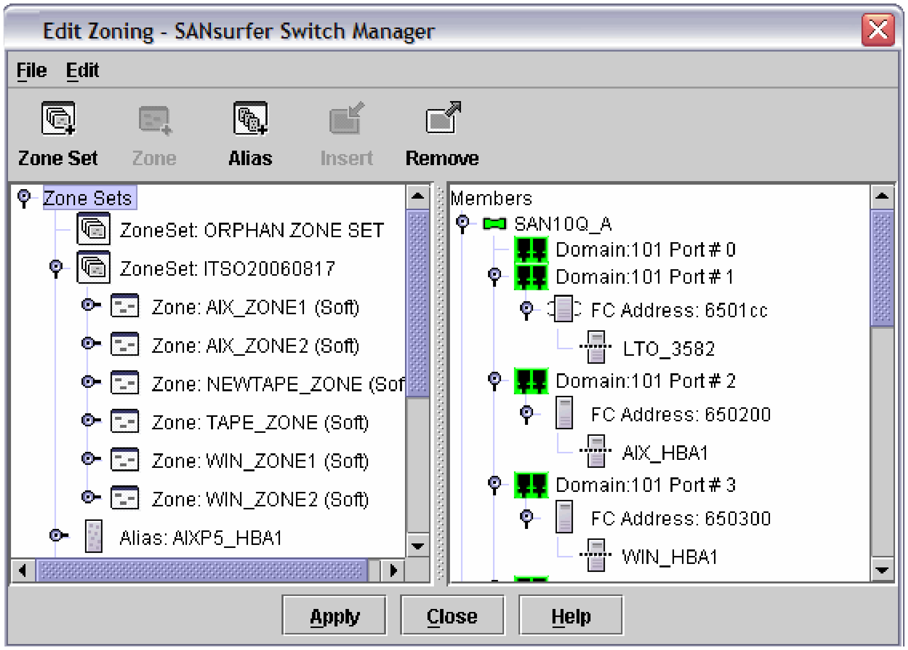

Edit Zoning - SANsurfer Switch Manager
File
Edit
Zone Set
Zone
Alias
Insert
Remove
Zone Sets
ZoneSet: ORPHAN ZONE SET
ZoneSet: ITSO20060817
Zone: AIX_ZONE1 (Soft)
Zone: AIX_ZONE2 (Soft)
Zone: NEWTAPE_ZONE (Sof
Zone: TAPE_ZONE (Soft)
Zone: WIN_ZONE1 (Soft)
Zone: WIN_ZONE2 (Soft)
Alias: AIXP5_HBA1
Members
SAN10Q_A
Domain:101 Port # 0
Domain:101 Port # 1
FC Address: 6501cc
LTO_3582
Domain:101 Port # 2
FC Address: 650200
AIX_HBA1
Domain:101 Port # 3
FC Address: 650300
WIN_HBA1
Apply
Close
Help

Figure 3-80 Edit zoning

As shown in Figure 3-81, we added a new zone to the active zone set, called *NEW_TAPE* in our example. We also added the members to this zoneset. To activate the change, select the **Apply** button and activate the same zone set.

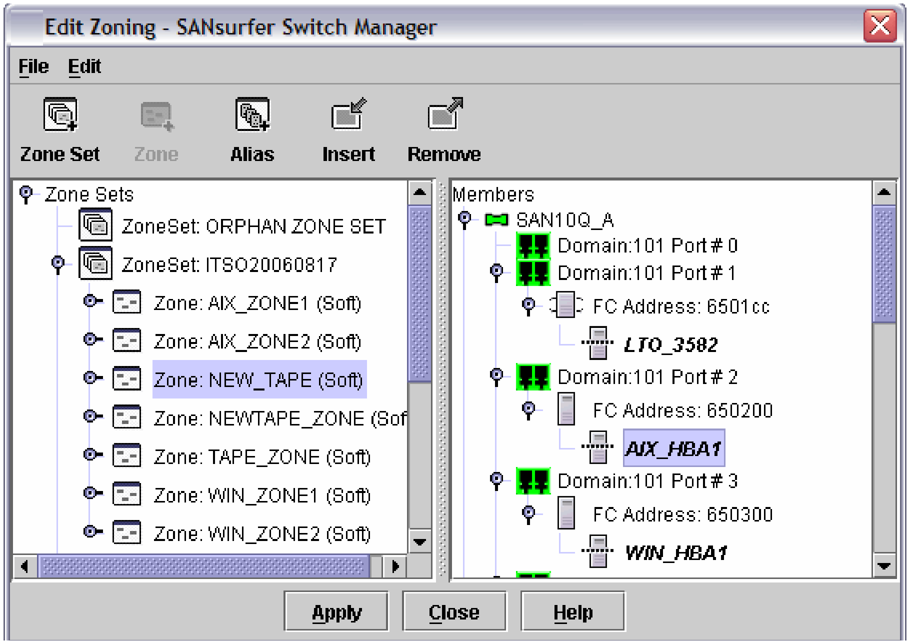

Edit Zoning - SANsurfer Switch Manager
File
Edit
Zone Set
Zone
Alias
Insert
Remove
Zone Sets
ZoneSet: ORPHAN ZONE SET
ZoneSet: ITSO20060817
Zone: AIX_ZONE1 (Soft)
Zone: AIX_ZONE2 (Soft)
Zone: NEW_TAPE (Soft)
Zone: NEWTAPE_ZONE (Sof
Zone: TAPE_ZONE (Soft)
Zone: WIN_ZONE1 (Soft)
Zone: WIN_ZONE2 (Soft)
Members
SAN10Q_A
Domain:101 Port # 0
Domain:101 Port # 1
FC Address: 6501cc
LTO_3582
Domain:101 Port # 2
FC Address: 650200
AIX_HBA1
Domain:101 Port # 3
FC Address: 650300
WIN_HBA1
Apply
Close
Help

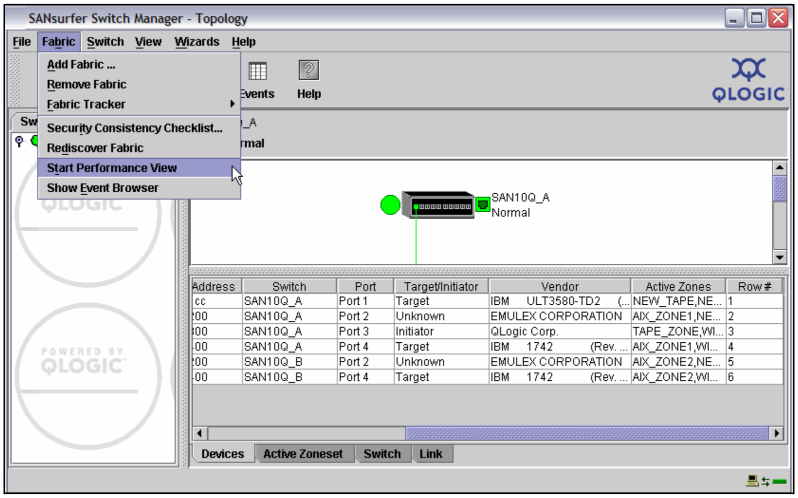
Figure 3-81 Zone addition

3.2.7 Performance Viewer

The Performance Viewer application is a separate application from the switch management application that displays port performance using graphs.

Performance Viewer provides a method to visually monitor the real-time traffic for each port on a switch. Traffic for a port is displayed in its own graph that is continually updated to reflect changes as they occur, and is based on the number of kilobytes (Kb), or on the number of frames that pass through that port per second.

To start Performance Viewer from within the topology display, select **Fabric** → **Start Performance Viewer**, as shown in Figure 3-82.


SANsurfer Switch Manager - Topology
File
Fabric
Switch
View
Wizards
Help
Add Fabric ...
Remove Fabric
Fabric Tracker
Security Consistency Checklist...
Rediscover Fabric
Start Performance View
Show Event Browser
Events
Help
QLOGIC
POWERED BY QLOGIC
SAN10Q_A
Normal
Devices
Active Zoneset
Switch
Link

Address	Switch	Port	Target/Initiator	Vendor	Active Zones	Row #
cc	SAN10Q_A	Port 1	Target	IBM ULT3580-TD2 (...	NEW_TAPE,NE...	1
00	SAN10Q_A	Port 2	Unknown	EMULEX CORPORATION	AIX_ZONE1,NE...	2
00	SAN10Q_A	Port 3	Initiator	QLogic Corp.	TAPE_ZONE,WI...	3
00	SAN10Q_A	Port 4	Target	IBM 1742 (Rev. ...	AIX_ZONE1,WI...	4
00	SAN10Q_B	Port 2	Unknown	EMULEX CORPORATION	AIX_ZONE2,NE...	5
00	SAN10Q_B	Port 4	Target	IBM 1742 (Rev. ...	AIX_ZONE2,WI...	6

Figure 3-82 Starting performance viewer

On the left side of the window is a list of ports available for monitoring. Click the port (or ports) that you wish to monitor, and a graphical view of this port appears in the right hand side of the window, as shown in Figure 3-83.

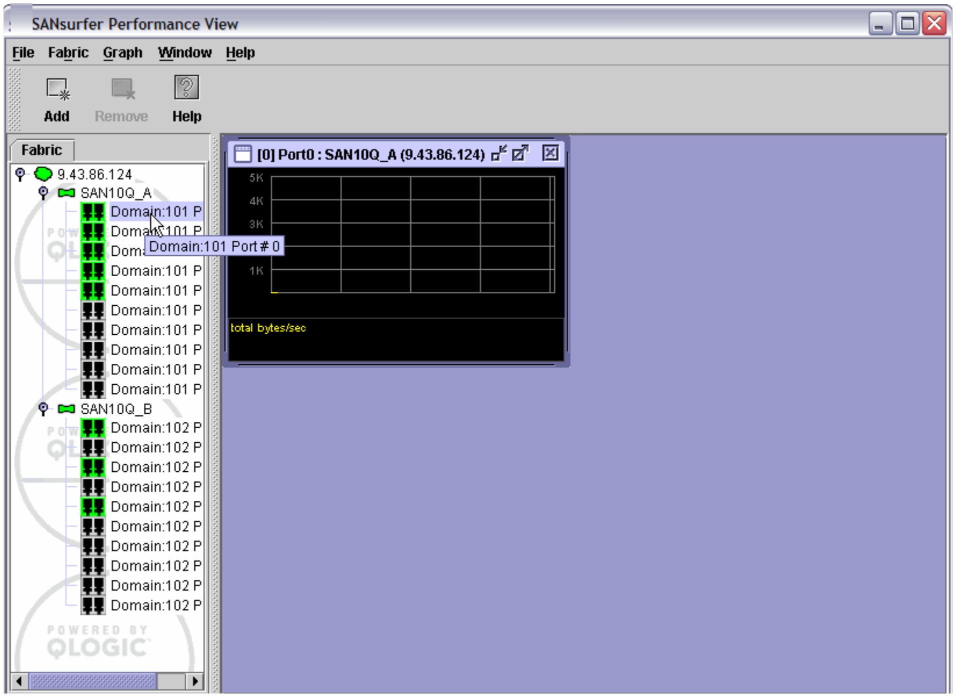
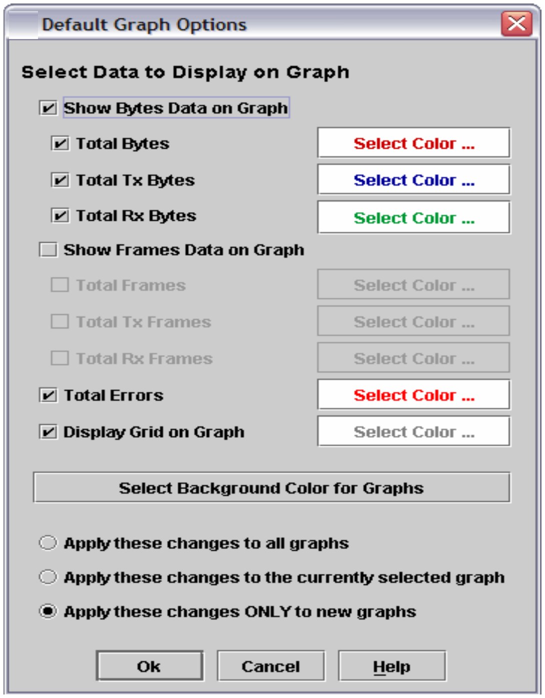

SANsurfer Performance View
File
Fabric
Graph
Window
Help
Add
Remove
Help
Fabric
9.43.86.124
SAN10Q_A
Domain:101 P
Domain:101 Port # 0
SAN10Q_B
Domain:102 P
[0] Port0 : SAN10Q_A (9.43.86.124)
5K
4K
3K
1K
total bytes/sec
POWERED BY QLOGIC

Figure 3-83   Performance view

Select **Graph** → **Modify Graph Options** from the tool bar. This opens the *Default Graph Options* dialog, shown in Figure 3-84. Here you can choose display options, which affect what is to be plotted and how the graphs are displayed.


Default Graph Options
Select Color ...
Select Color ...
Select Color ...
Select Color ...
Select Color ...
Select Color ...
Select Color ...
Select Color ...
Select Background Color for Graphs
Ok
Cancel
Help

Select Data to Display on Graph

☑ Show Bytes Data on Graph
- ☑ Total Bytes
- ☑ Total Tx Bytes
- ☑ Total Rx Bytes

☐ Show Frames Data on Graph
- ☐ Total Frames
- ☐ Total Tx Frames
- ☐ Total Rx Frames

☑ Total Errors

☑ Display Grid on Graph

○ Apply these changes to all graphs
○ Apply these changes to the currently selected graph
● Apply these changes ONLY to new graphs

Figure 3-84 Default graph options.

You can select to display the following data:

- Display either Frames Data or Byte Data on the Graph. These can be plotted as one or all of the following, and you can also choose the color scheme for the graph:
  - Total frames/bytes transmitted and received (Total Frames/Bytes)
  - Total frames/bytes transmitted (Total Tx Frames/Bytes)
  - Total frames/bytes received (Total Rx Frames/Bytes)
- Display total errors, by clicking the Total Errors check box.
- Display or hide the unit grid. Click the Display Grid on Graph check box to display the unit grid.
- Set your Default Graph Options.
- Select one option and click an **OK** button to apply the color scheme changes to all graphs, to the currently selected graph, or to only new graphs.

Figure 3-85 shows an example of monitoring four ports; this includes monitoring E ports.

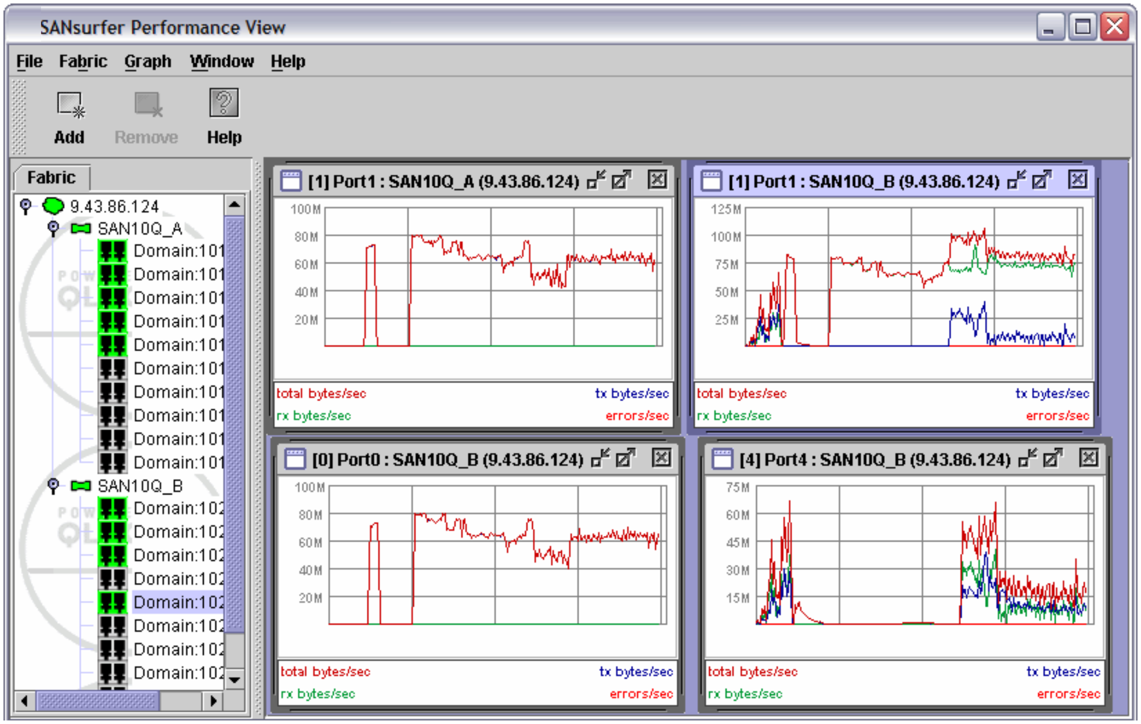

SANsurfer Performance View
File
Fabric
Graph
Window
Help
Add
Remove
Help
Fabric
9.43.86.124
SAN10Q_A
Domain:101
Domain:101
Domain:101
Domain:101
Domain:101
Domain:101
Domain:101
Domain:101
Domain:101
Domain:101
SAN10Q_B
Domain:102
Domain:102
Domain:102
Domain:102
Domain:102
Domain:102
Domain:102
Domain:102
[1] Port1 : SAN10Q_A (9.43.86.124)
100M
80M
60M
40M
20M
total bytes/sec
tx bytes/sec
rx bytes/sec
errors/sec
[1] Port1 : SAN10Q_B (9.43.86.124)
125M
100M
75M
50M
25M
total bytes/sec
tx bytes/sec
rx bytes/sec
errors/sec
[0] Port0 : SAN10Q_B (9.43.86.124)
100M
80M
60M
40M
20M
total bytes/sec
tx bytes/sec
rx bytes/sec
errors/sec
[4] Port4 : SAN10Q_B (9.43.86.124)
75M
60M
45M
30M
15M
total bytes/sec
tx bytes/sec
rx bytes/sec
errors/sec

Figure 3-85 Performance line graph

Figure 3-86 shows an example of monitoring four ports using bar graphs, this includes monitoring E_Ports.

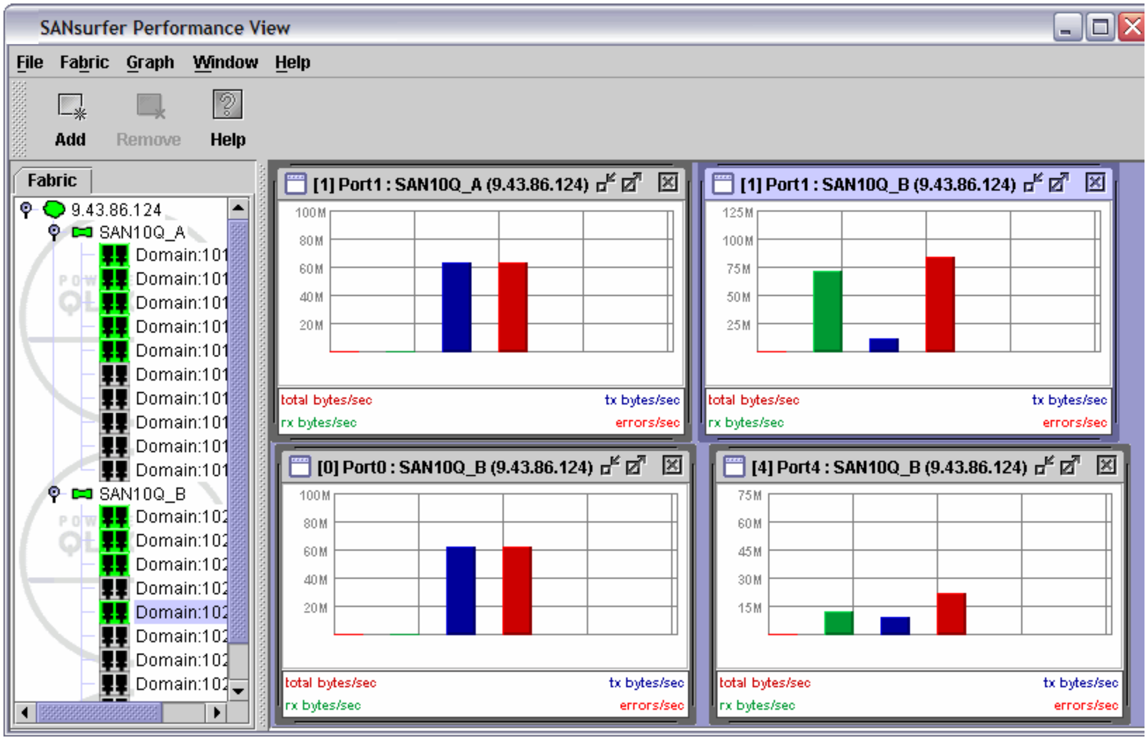

SANsurfer Performance View
File Fabric Graph Window Help
Add
Remove
Help
Fabric
9.43.86.124
SAN10Q_A
Domain:101
SAN10Q_B
Domain:102
[1] Port1 : SAN10Q_A (9.43.86.124)
[1] Port1 : SAN10Q_B (9.43.86.124)
[0] Port0 : SAN10Q_B (9.43.86.124)
[4] Port4 : SAN10Q_B (9.43.86.124)
100M
80M
60M
40M
20M
125M
75M
50M
25M
45M
30M
15M
total bytes/sec
tx bytes/sec
rx bytes/sec
errors/sec

Figure 3-86 Performance bar graph

To change your view from bar graph to line graph, select **Graph** → **Set Global Graph Type**.

By selecting **File** → **Save Current Graph Statistics to file** from the performance view menu shown in Figure 3-87, you get the option to save a single graph to a file, or by selecting **File** → **Save All Graph Statistics to file**, you can save all graphs currently being monitored. This data is saved as a .csv file.

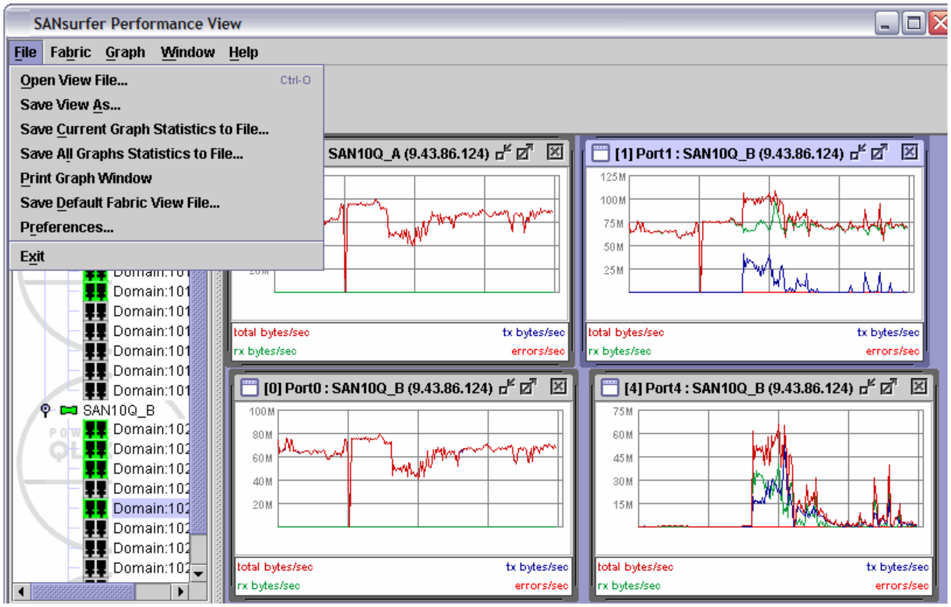

SANsurfer Performance View
File
Fabric
Graph
Window
Help
Open View File... Ctrl-O
Save View As...
Save Current Graph Statistics to File...
Save All Graphs Statistics to File...
Print Graph Window
Save Default Fabric View File...
Preferences...
Exit
Domain:101
SAN10Q_B
Domain:102
SAN10Q_A (9.43.86.124)
[1] Port1 : SAN10Q_B (9.43.86.124)
[0] Port0 : SAN10Q_B (9.43.86.124)
[4] Port4 : SAN10Q_B (9.43.86.124)
125M
100M
75M
50M
25M
80M
60M
40M
20M
45M
30M
15M
total bytes/sec
tx bytes/sec
rx bytes/sec
errors/sec

Figure 3-87 Saving performance data to file.

By default, the polling frequency is set to one second. You can change this by selecting **Graph** → **Set Polling Frequency**. This option window is displayed in Figure 3-88.

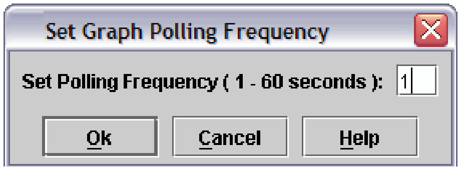

Set Polling Frequency (1 - 60 seconds): 1
Set Graph Polling Frequency
Ok
Cancel
Help

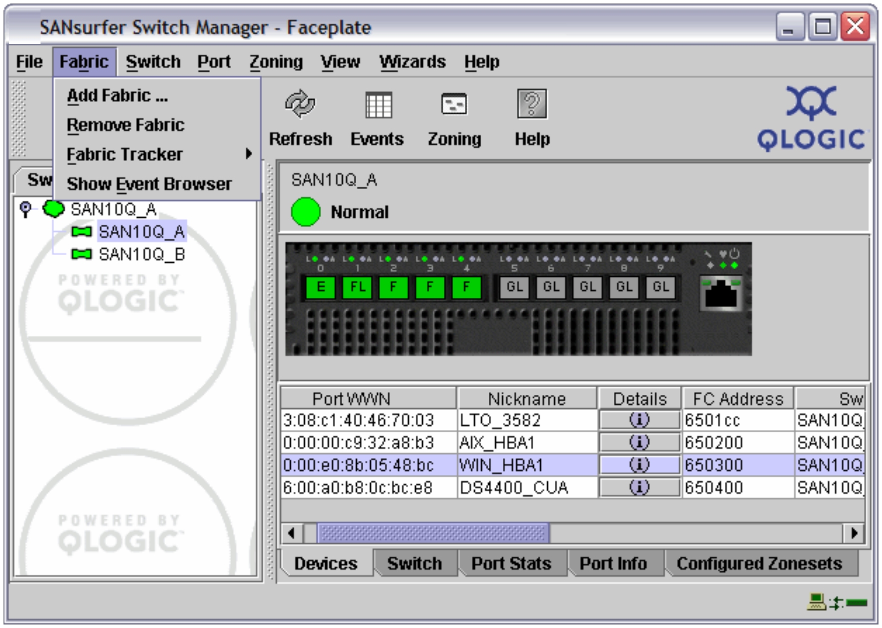
Figure 3-88 Polling Frequency

3.2.8 Logs and troubleshooting

In these topics we show the logs and some basic troubleshooting information.

Event Browser

The Event Browser displays a list of events generated by all the switches in the fabric, as well as the switch management application. Events that are generated by the application are not saved on the switch, but can be saved to a file during the switch management session. To display the Event Browser, select **Fabric** → **Show Event Browser** as shown in Figure 3-89.

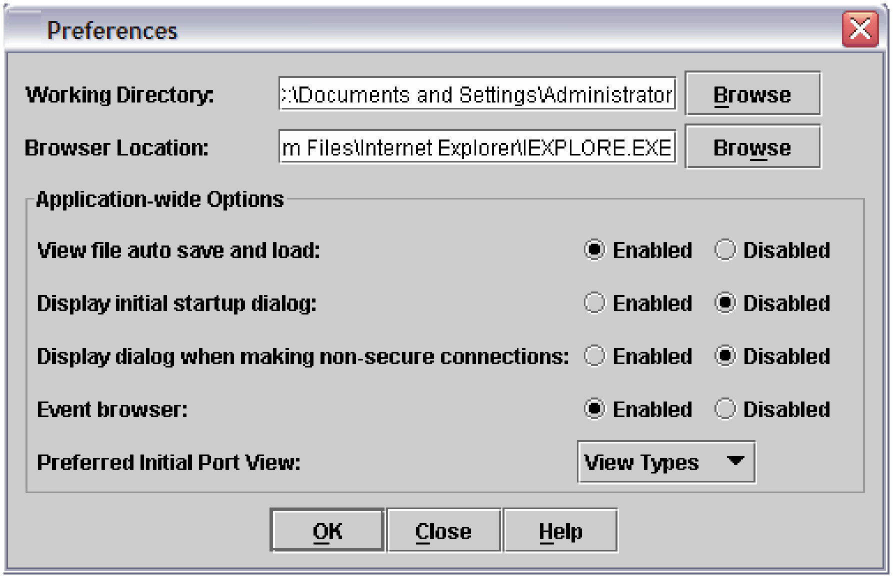

SANsurfer Switch Manager - Faceplate
File
Fabric
Switch
Port
Zoning
View
Wizards
Help
Add Fabric ...
Remove Fabric
Fabric Tracker
Show Event Browser
Refresh
Events
Zoning
Help
QLOGIC
Sw
SAN10Q_A
SAN10Q_A
SAN10Q_B
POWERED BY QLOGIC
POWERED BY QLOGIC
SAN10Q_A
Normal
0
1
2
3
4
5
6
7
8
9
E
FL
F
F
F
GL
GL
GL
GL
GL
Devices
Switch
Port Stats
Port Info
Configured Zonesets

Port WWN	Nickname	Details	FC Address	Sw
3:08:c1:40:46:70:03	LTO_3582	ⓘ	6501cc	SAN10Q
0:00:00:c9:32:a8:b3	AIX_HBA1	ⓘ	650200	SAN10Q
0:00:e0:8b:05:48:bc	WIN_HBA1	ⓘ	650300	SAN10Q
6:00:a0:b8:0c:bc:e8	DS4400_CUA	ⓘ	650400	SAN10Q

Figure 3-89 Event Browser selection

If you cannot select the event browser option, you might have to enable the Show Event Browser option in the Fabric menu. Select **File** → **Preferences**, and from the window shown in Figure 3-90, enable the Event Browser.

> **Note:** If the Event Browser is enabled using the Preferences dialog, the next time the application is started, all events from the switch alarm log are displayed. If the Event Browser is disabled when the application is started and later enabled, only those events from the time the Event Browser was enabled and forward from that time are displayed.



Working Directory: :\Documents and Settings\Administrator

Browser Location: m Files\Internet Explorer\IEXPLORE.EXE

Application-wide Options

View file auto save and load: ● Enabled ○ Disabled

Display initial startup dialog: ○ Enabled ● Disabled

Display dialog when making non-secure connections: ○ Enabled ● Disabled

Event browser: ● Enabled ○ Disabled

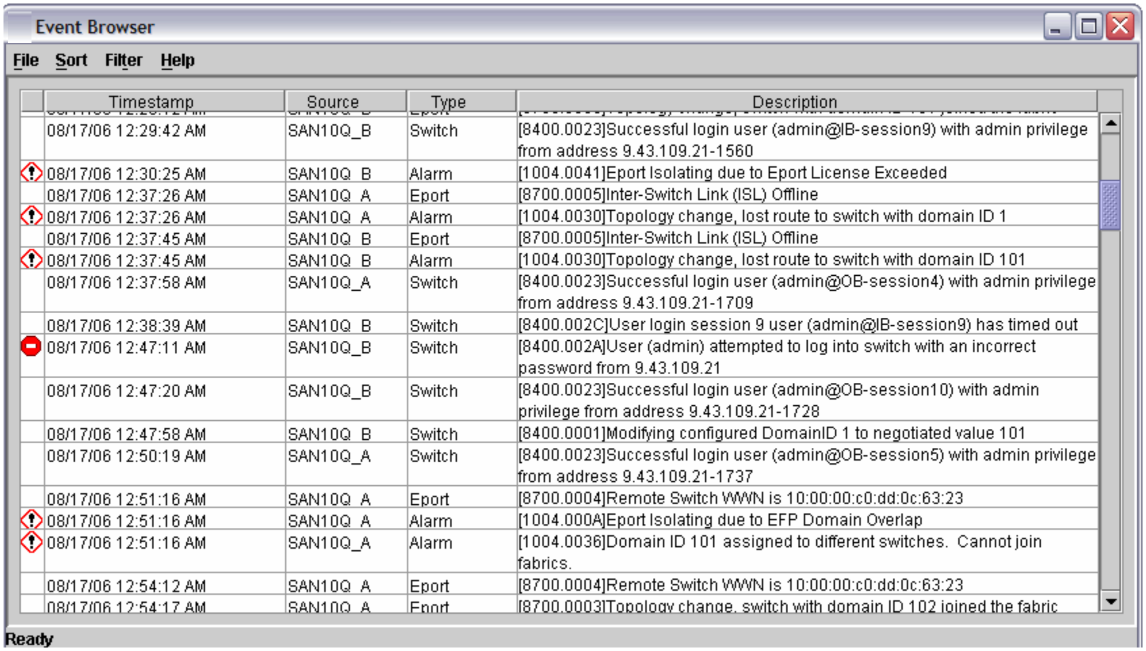
Preferred Initial Port View: View Types

Figure 3-90 Preferences.

Entries in the Event Browser, as shown in Figure 3-91, are formatted by severity, time stamp, source, type, and description. The maximum number of entries allowed in the Event Browser is 10,000. The maximum number of entries allowed on a switch is 1200. When the maximum is reached, the event list wraps and the oldest events are discarded. The switch uses the switch time stamp, while event entries generated by the application have the workstations time stamp.

To save or export the events to a file during a session, select **File** → **Save As**, and enter a name for the XML file.

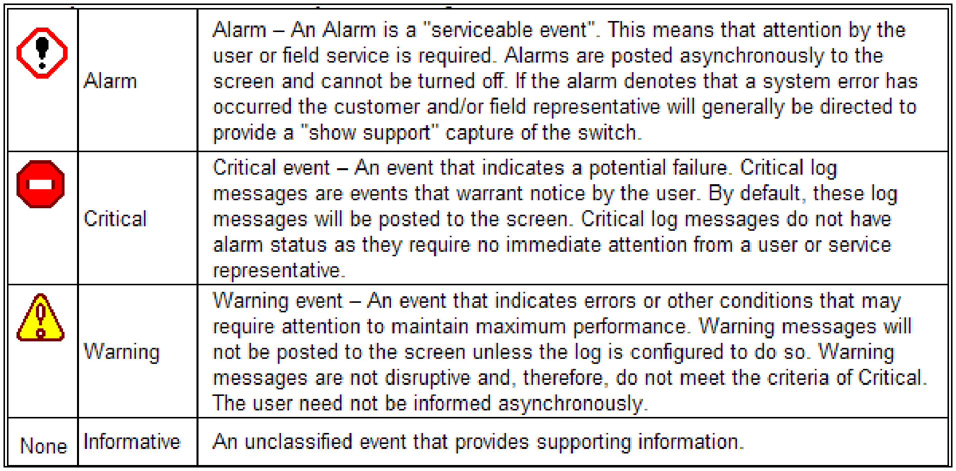
From the event browser you can get important information regarding the status of your switch or fabric. The event browser gives you detailed information regarding any errors that have occurred.



	Timestamp	Source	Type	Description
	08/17/06 12:29:42 AM	SAN10Q_B	Switch	[8400.0023]Successful login user (admin@IB-session9) with admin privilege from address 9.43.109.21-1560
◈	08/17/06 12:30:25 AM	SAN10Q_B	Alarm	[1004.0041]Eport Isolating due to Eport License Exceeded
	08/17/06 12:37:26 AM	SAN10Q_A	Eport	[8700.0005]Inter-Switch Link (ISL) Offline
◈	08/17/06 12:37:26 AM	SAN10Q_A	Alarm	[1004.0030]Topology change, lost route to switch with domain ID 1
	08/17/06 12:37:45 AM	SAN10Q_B	Eport	[8700.0005]Inter-Switch Link (ISL) Offline
◈	08/17/06 12:37:45 AM	SAN10Q_B	Alarm	[1004.0030]Topology change, lost route to switch with domain ID 101
	08/17/06 12:37:58 AM	SAN10Q_A	Switch	[8400.0023]Successful login user (admin@OB-session4) with admin privilege from address 9.43.109.21-1709
	08/17/06 12:38:39 AM	SAN10Q_B	Switch	[8400.002C]User login session 9 user (admin@IB-session9) has timed out
⛔	08/17/06 12:47:11 AM	SAN10Q_B	Switch	[8400.002A]User (admin) attempted to log into switch with an incorrect password from 9.43.109.21
	08/17/06 12:47:20 AM	SAN10Q_B	Switch	[8400.0023]Successful login user (admin@OB-session10) with admin privilege from address 9.43.109.21-1728
	08/17/06 12:47:58 AM	SAN10Q_B	Switch	[8400.0001]Modifying configured DomainID 1 to negotiated value 101
	08/17/06 12:50:19 AM	SAN10Q_A	Switch	[8400.0023]Successful login user (admin@OB-session5) with admin privilege from address 9.43.109.21-1737
	08/17/06 12:51:16 AM	SAN10Q_A	Eport	[8700.0004]Remote Switch WWN is 10:00:00:c0:dd:0c:63:23
◈	08/17/06 12:51:16 AM	SAN10Q_A	Alarm	[1004.000A]Eport Isolating due to EFP Domain Overlap
◈	08/17/06 12:51:16 AM	SAN10Q_A	Alarm	[1004.0036]Domain ID 101 assigned to different switches. Cannot join fabrics.
	08/17/06 12:54:12 AM	SAN10Q_A	Eport	[8700.0004]Remote Switch WWN is 10:00:00:c0:dd:0c:63:23
	08/17/06 12:54:17 AM	SAN10Q_A	Eport	[8700.0003]Topology change, switch with domain ID 102 joined the fabric

Figure 3-91 Event Browser

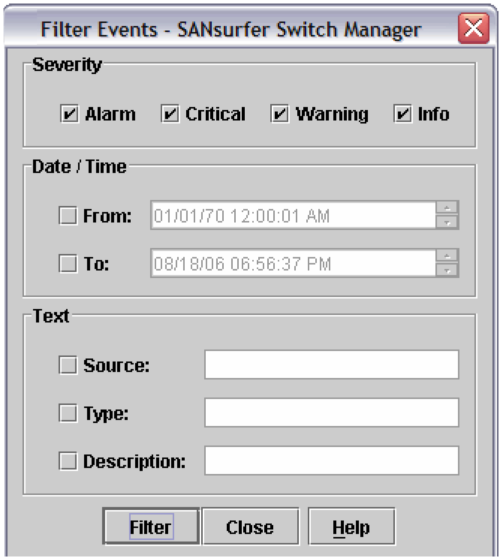
Severity is indicated in the severity column using icons. The meanings of these icons and their severity are shown in Figure 3-92.



◈	Alarm	Alarm – An Alarm is a "serviceable event". This means that attention by the user or field service is required. Alarms are posted asynchronously to the screen and cannot be turned off. If the alarm denotes that a system error has occurred the customer and/or field representative will generally be directed to provide a "show support" capture of the switch.
⛔	Critical	Critical event – An event that indicates a potential failure. Critical log messages are events that warrant notice by the user. By default, these log messages will be posted to the screen. Critical log messages do not have alarm status as they require no immediate attention from a user or service representative.
⚠	Warning	Warning event – An event that indicates errors or other conditions that may require attention to maintain maximum performance. Warning messages will not be posted to the screen unless the log is configured to do so. Warning messages are not disruptive and, therefore, do not meet the criteria of Critical. The user need not be informed asynchronously.
None	Informative	An unclassified event that provides supporting information.

Figure 3-92 Event Severity Levels and Icons

Filtering the Event Browser enables you to display only those events that are of interest based on the event severity, timestamp, source, type, and description. To filter the Event Browser, select **Filter** → **Filter** to open the Filter Events dialog, shown in Figure 3-93. The filter does not remove the events from the browser.



Severity

☑ Alarm ☑ Critical ☑ Warning ☑ Info

Date / Time

☐ From: 01/01/70 12:00:01 AM

☐ To: 08/18/06 06:56:37 PM

Text

☐ Source:

☐ Type:

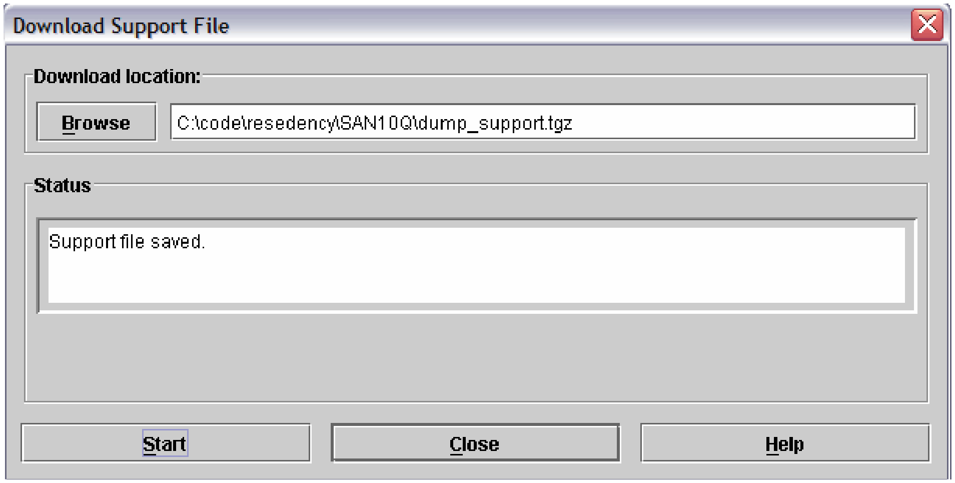
☐ Description:

Figure 3-93 Filter events dialog

Support files

The Download Support File menu option assembles all log files and switch memory data into a core dump file (dump_support.tgz). This file can be sent to technical support personnel for troubleshooting switch problems.

From SANsurfer, select the switch for which this is required. Then from the Faceplate menu, select **Switch** → **Download Support File.** You then select the desired location on your work station, and the name of the file you wish to save using the **Browse** button. Click the **Start** button and the file is saved to your workstation, as shown in Figure 3-94.



C:\code\resedency\SAN10Q\dump_support.tgz

Support file saved.

Figure 3-94 Support file download

Switch Reset

There are three ways to reset a switch, as shown in Figure 3-95:

- Hot reset. This resets a switch without a power-on self-test. This reset activates the pending firmware, but does not disrupt switch traffic. If errors are detected on a port during a hot reset, the port is reset automatically.
- Reset. This resets a switch without a power-on self test. This reset activates the pending firmware and it is disruptive to switch traffic.
- Hard reset. This resets a switch with a power-on self test. This reset activates the pending firmware and it is disruptive to switch traffic.

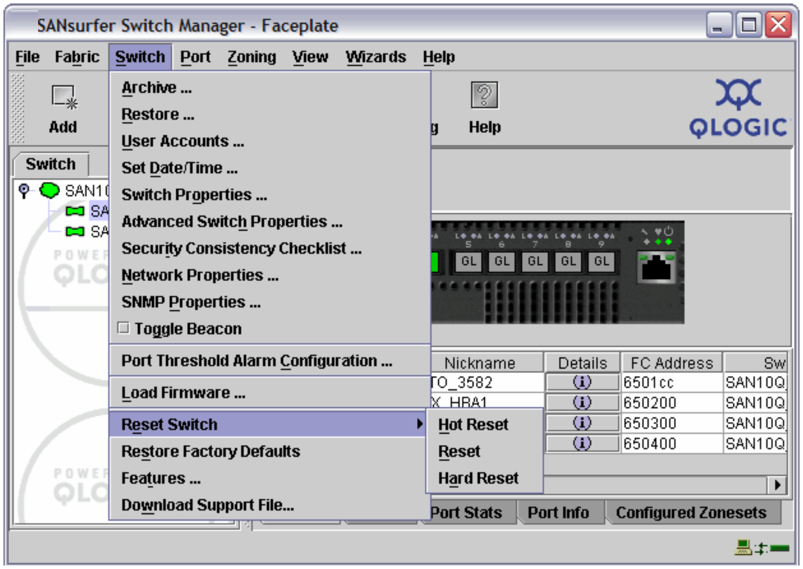

SANsurfer Switch Manager - Faceplate
File
Fabric
Switch
Port
Zoning
View
Wizards
Help
Add
Help
QLOGIC
Archive ...
Restore ...
User Accounts ...
Set Date/Time ...
Switch Properties ...
Advanced Switch Properties ...
Security Consistency Checklist ...
Network Properties ...
SNMP Properties ...
☐ Toggle Beacon
Port Threshold Alarm Configuration ...
Load Firmware ...
Reset Switch
Restore Factory Defaults
Features ...
Download Support File...
Hot Reset
Reset
Hard Reset
Nickname
Details
FC Address
6501cc
650200
650300
650400
Port Stats
Port Info
Configured Zonesets

Figure 3-95 Switch reset

Maintenance mode

If there is a requirement to reset any switch setting to default, such as IP address or password, perform the following procedure using Maintenance mode.

Maintenance mode temporarily returns the switch IP address to 10.0.0.1 and provides opportunities to perform the following tasks:

- Unpack a firmware image file.
- Restore the network configuration parameters to the default values.
- Remove all user accounts and restore the Admin account name password to the default.
- Copy the log file.
- Restore factory defaults for all but user accounts and zoning.
- Restore all switch configuration parameters to the factory default values.
- Reset the switch.
- Update the system boot loader.

To place the switch in Maintenance mode, perform the following steps:

1. Press and hold the maintenance button with a pointed tool, as indicated by the white arrow in Figure 3-96.
2. All LEDs light up; wait until *only* the heartbeat LED is lit, and release the button.

3. Establish a Telnet session with the switch by using the Maintenance mode IP address 10.0.0.1, using a crossover cable to your workstation.
4. Enter the Maintenance mode account name *prom* and password *prom*, and press Enter:

   ```
   Switch login: prom
   Password:xxxx
   ```

   The following menu is displayed, as shown in Example 3-1.

Example 3-1 Account name and password

```
0) Exit
1) Image Unpack
2) Reset Network Config
3) Reset User Accounts to Default
4) Copy Log Files
5) Remove Switch Config
6) Remake Filesystem
7) Reset Switch
8) Update Boot Loader Option
```

5. You can now select a switch recovery option. Type the number corresponding to the option you wish to select, and press Enter.

Front panel

On the front panel we have three status LEDs.

- The input power LED, which indicates the voltage status of the switch
- A heartbeat LED, which indicates the status of the internal switch processor and the results of the power-on self-test
- A system fault LED, which indicates an over temperature condition or a POST error.

We also have a reset button indicated by the white arrow in Figure 3-96.

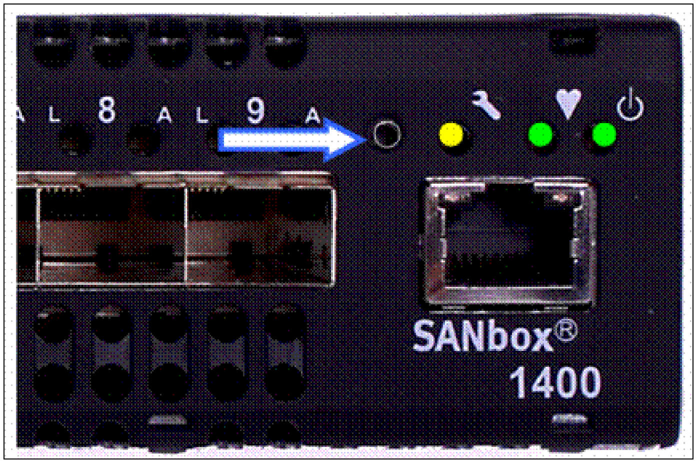


Figure 3-96 Front panel

LED diagnostics

In the following topics we describe the LED conditions.

Input Power LED

The input power LED is lit when the Fibre Channel switch logic circuitry is receiving the correct voltages. If the input power LED is off, complete the following steps:

1. Inspect the power cords and connectors. Is the cord disconnected or is the cord or connector damaged?
2. Inspect the ac power source. Is the power source delivering the correct voltage?
3. If the condition remains, contact your technical support representative.

System fault LED

The system fault LED is lit when the Fibre Channel switch logic circuitry is overheating or when there is a POST error. The system fault LED is always accompanied by a heartbeat LED error flash code. If the system fault LED is lit, identify the heartbeat LED error flash pattern, and take the necessary actions.

Heartbeat LED

The heartbeat LED indicates the operational status of the Fibre Channel switch. When the POST is completed with no errors, the heartbeat LED flashes at a steady rate of once per second.

When the Fibre Channel switch is in Maintenance mode, the heartbeat LED is lit continuously. All other flash patterns indicate critical errors.

- 2 flashes - Internal firmware failure flash pattern
- 3 flashes - System error flash pattern
- 4 flashes - Configuration file system error flash pattern
- 5 flashes - Over temperature flash pattern

Port Logged-in LED

Above each port is the port logged-in LED. This LED has the following three indications:

- Lit continuously — this means that a device is logged in to the port.
- Flashing once per second — this means that a device is busy logging in to the port.
- Flashing twice per second — this means the port is down or offline, or an error has occurred. If a port logged-in LED is flashing twice per second, review the event browser for alarm messages about the affected port. You can also inspect the alarm log by using the Show Alarm command.

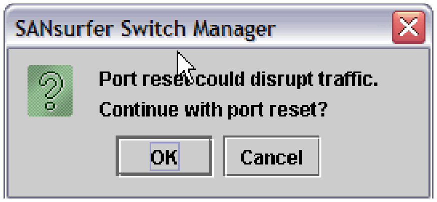
Note: For more detailed information regarding these LEDs, refer to Chapter 5 of the *System Storage SAN10Q 4 Gbps 10-Port Fibre Channel SwitchType 6918 Installation Guide,* 31R1632, on the CD supplied with the switch.

Port testing

The following topics cover the ways to test a port.

Resetting a port

The Reset Port option re-initializes the port using the saved configuration. From the Faceplate window, select the port(s) to be reset, then select **Port** → **Reset Port**. You get the confirmation message as shown in Figure 3-97. Click **OK** to reset the port.



Port reset could disrupt traffic.
Continue with port reset?

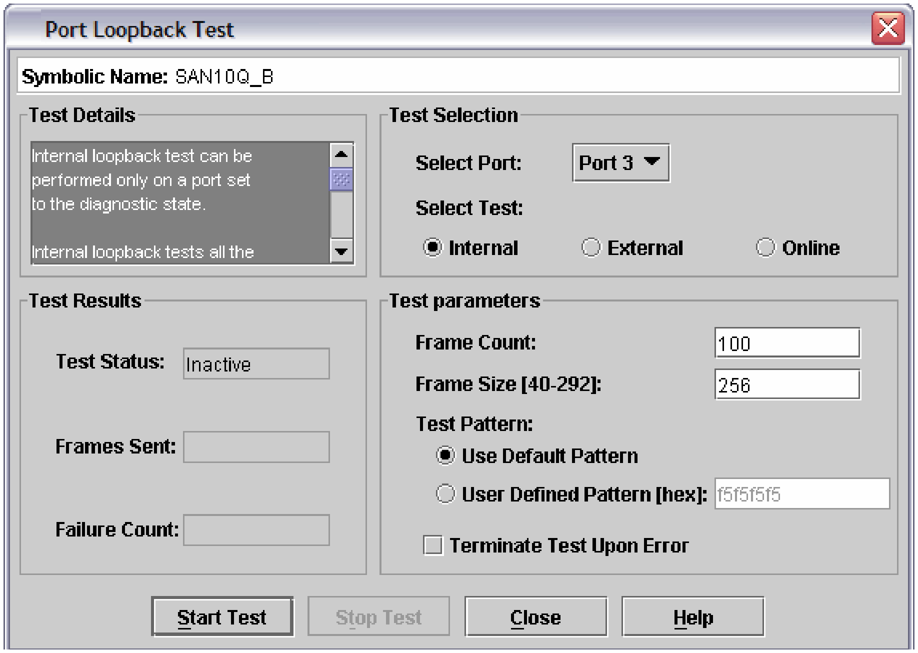
Figure 3-97 Resetting port

Testing ports

The port loopback tests verify correct port operation by sending a frame out through the loop, and then verifying that the frame received matches the frame that was sent. Only one port can be tested at a time for each type of test.

To run the internal, external, or online port loopback test on a port, select **Port** → **Port Loopback test**, the window shown in Figure 3-98 is now displayed. From this window, you have the following panels available:

- *Test Selection area:* Here you can choose type of loopback test to be run and select the port number:
  - **Internal:** The internal test sends a test frame from the ASIC through the SerDes chip and back to the ASIC for the selected ports. The port passes the test if the frame that was sent by the ASIC matches the test frame that was received. This test requires that the port be in diagnostics mode, and is therefore disruptive.



Symbolic Name: SAN10Q_B

Internal loopback test can be performed only on a port set to the diagnostic state.

Internal loopback tests all the

Select Port: Port 3

Select Test:

● Internal ○ External ○ Online

Test Status: Inactive

Frames Sent:

Failure Count:

Frame Count: 100

Frame Size [40-292]: 256

Test Pattern:

● Use Default Pattern

○ User Defined Pattern [hex]: f5f5f5f5

☐ Terminate Test Upon Error

Figure 3-98 Port loopback test

  - **External:** The external test sends a test frame from the ASIC through the SerDes chip, through the SFP module fitted with an external loopback plug, as shown in Figure 3-99, and back to the ASIC for the selected ports. The port passes the test if the test frame that was sent by the ASIC matches the test frame that was received. This test requires that the port be in diagnostics mode, and is therefore disruptive.

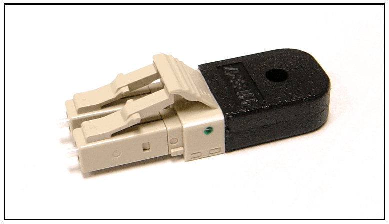
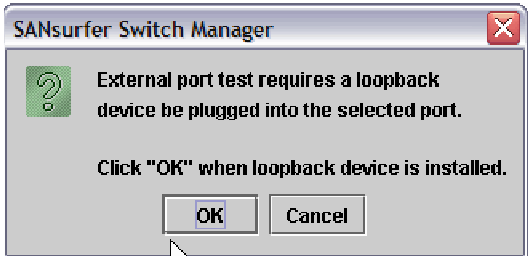


Figure 3-99 External loopback plug

  - **Online:** The online test verifies communications between the port and its device node or device loop. The port being tested must be online and connected to a remote device. The port passes the test if the frame that was sent by the ASIC matches the frame that was received. This test does not disrupt communication on the selected port.

- Test Parameters:
  - Enter the frame count.
  - Enter the frame size.
  - Enter the test pattern. You can use the default pattern or enter an 8-digit pattern (hex). For online test, you can select the Terminate Test Upon Error check box if you want the test to stop should it encounter an error. 5. You click **Start Test** to begin the test. The Test Results area shows the test status, number of frames sent, and number of errors found.

Click **Start Test**, as shown in Figure 3-98 on page 722, to begin the test. You get a window like the one shown here in Figure 3-100; read this message and click **OK**. Then observe the results in the Test Results area of the window shown in Figure 3-98 on page 722.



External port test requires a loopback device be plugged into the selected port.

Click "OK" when loopback device is installed.

Figure 3-100 Start test dialog

Take the necessary actions based on the resultant feedback. If necessary, contact technical support for diagnostic help.

4

Implementing a SAN with the Cisco family

In this chapter we introduce the Cisco MDS 9000 family of Fibre Channel switches and enterprise directors. We describe the initial setup required to activate the Cisco Fabric Manager client GUI, and describe how to configure the Cisco SAN with the GUI.

Note: We used a pre-GA version of the Cisco Multilayer intelligent SAN operating system (SAN-OS) Version 3.x for all our examples and testing.
If your SAN-OS level is different, some of the panels might not look the same. However, the concepts introduced here should still apply.

© Copyright IBM Corp. 1999-2007. All rights reserved.

4.1 Product introduction

The Cisco MDS 9000 family provides midrange switches and enterprise directors. In the following sections, we briefly describe each model, then present a summary in Table 4-1 on page 729.

4.1.1 MDS 9020 Fabric Switch (non-modular)

This switch provides 4-20 ports, 4 Gbps fabric switching for open systems, and is designed to address the requirements of small and medium-sized businesses with a wide range of SAN capabilities. It can be used as part of SAN solutions from simple single-switch configurations to larger multi-switch configurations in support of simplification and advanced business continuity capabilities.

4.1.2 MDS 9120 Multilayer Fabric Switch (non-modular)

This switch provides 4-20 ports, 2 Gbps fabric switching for open systems, infrastructure simplification and business continuity solutions. The base switch offers 4 “target-optimized” ports and 16 “host-optimized” ports, Virtual SAN (VSAN), and Cisco Fabric Manager.

4.1.3 MDS 9140 Multilayer Fabric Switch (non-modular)

This switch provides 4-40 ports, 2 Gbps fabric switching for open systems, infrastructure simplification, and business continuity solutions. The base switch offers 8 “target-optimized” ports and 32 “host-optimized” ports, Virtual SAN (VSAN) and Cisco Fabric Manager.

4.1.4 MDS 9216(a/i) Multilayer Fabric Switch

This switch provides 16-port, 2 Gbps fabric switching for open systems, infrastructure simplification, and business continuity solutions. The base switch offers 16 Fibre Channel ports (model A), or 14 Fibre Channel and 2-IP ports (model i), Virtual SAN (VSAN) and Cisco Fabric Manager. Features include 14 Fibre Channel and 2 IP port, 4-port and 8-port IPS Modules with iSCSI and FCIP capabilities, 16-port and 32-port FC Switch Modules, 32-port FC Switch Module with “host-optimized” ports, Caching Services Module for IBM SAN Volume Controller Software, and Mainframe Package for 16 or 32 port FICON switching.

4.1.5 MDS 9506 Multilayer Director

The director provides 16-128 ports, 2 Gbps fabric switching for open systems and 16-64 port FICON switching for mainframe, infrastructure simplification and business continuity solutions. The base director offers Virtual SAN (VSAN), Cisco Fabric Manager and four feature slots. Features include 14 Fibre Channel and 2 IP ports, 4-port and 8-port IPS Modules with iSCSI and FCIP capabilities, 16-port FC Switch Module, 16-port and 32-port FC Switch Modules with "host-optimized" ports, Caching Services Module for IBM SAN Volume Controller Software, and Mainframe Package for FICON switching. It also supports 4 Gbps and 10 Gbps Fibre Channel modules.

4.1.6 MDS 9509 Multilayer Director

The director provides 32-224 ports, 2 Gbps fabric switching for open systems and 32-112 port FICON switching for mainframe, infrastructure simplification, and business continuity solutions. The base director offers Virtual SAN (VSAN), Cisco Fabric Manager and feature slots. Features include 14 Fibre Channel and 2 IP ports, 4-port and 8-port IPS Modules with iSCSI and FCIP capabilities, 16-port and 32-port FC Switch Modules with "host-optimized" ports, Caching Services Module for IBM SAN Volume Controller Software, and Mainframe Package for FICON switching. It also supports 4 Gbps and 10 Gbps Fibre Channel modules.

4.1.7 MDS 9513 Multilayer Director

The Cisco MDS 9513 Multilayer Director (IBM 2062-E11) combines increased scalability and performance, intelligent SAN services, non-disruptive software upgrades, stateful process restart and failover, and full redundant operation in director-class SAN switching. Supporting up to 528 Fibre Channel ports in a single chassis and 2.1 Tbps of system bandwidth, the Cisco MDS 9513 is designed to meet the requirements of even the largest data center storage environments.

The main features of the Cisco MDS 9513 Multilayer Director are as follows:

- New Switching modules for Cisco MDS 9513 Multilayer Director (IBM 2062-E11):
  - 12-Port 1/2/4 Gbps Fibre Channel Switching module
  - 24-Port 1/2/4 Gbps Fibre Channel Switching module
  - 48-Port 1/2/4 Gbps Fibre Channel Switching module
  - 4-Port 10 Gbps Fibre Channel Switching module

- 1, 2, and 4 Gbps and 10 Gbps fibre channel switching with full bandwidth redundancy delivers highly available Fibre Channel performance with fully redundant bandwidth. Each crossbar module offers full system bandwidth so that the loss or removal of a single crossbar module does not impact system performance. It ensures 100% system throughput even in the event of a crossbar failure.
- MDS 9513 also supports the following existing MDS 9000 modules:
  - 16-Port 2 Gbps Fibre Channel Line Card
  - 32-Port 2 Gbps Fibre Channel Line Card
  - Storage Services Module
  - Multiprotocol Services Module
  - 8-Port IP Services Line Card
- The multilayer (multiprotocol and multi-transport) architecture of the Cisco MDS 9000 family enables a consistent feature set over a protocol-agnostic switch fabric. The MDS 9513 chassis transparently integrates Fibre Channel, FICON, SCSI over IP (iSCSI), and Fibre Channel over IP (FCIP) in one system. The flexible architecture of the MDS 9000 family also allows for seamless integration of future storage protocols.
- Integrated support for VSAN technology:
  - Access control lists ACLs) for hardware-based intelligent frame processing
  - Advanced traffic management features such as Fibre Channel Congestion Control FCC)
  - Fabric-wide quality of service (QoS) to enable migration from SAN islands to enterprise-wide storage networks
- Integrated hardware-based Virtual SANs (VSANs) and inter-VSAN routing that enables deployment of large-scale, multi-site, heterogeneous SAN topologies. Integration into port-level hardware allows any port within a system or fabric to be partitioned into any VSAN. Integrated hardware-based Inter-VSAN routing provides line-rate routing between any ports within a system or fabric without the necessity for external routing appliances.
- Advanced FICON services supporting 1, 2, and 4 Gbps FICON environments, including:
  - Cascaded FICON fabrics
  - VSAN-enabled intermix of mainframe and open systems environments
  - N_Port ID Virtualization for mainframe Linux partitions
  - CUP support enables in-band management of MDS 9000 family switches from the mainframe management console

Table 4-1 Cisco MDS 9000 family

Switch model	Slots available for switch modules (line cards)	Number of supervisor modules	Max number of FC ports
MDS 9020	NA (fixed configuration)		20
MDS 9120	NA (fixed configuration)		20
MDS 9140	NA (fixed configuration)		40
MDS 9216 (A/i)	1	1 (includes 16 FC ports or 14 + 2 GigE)	64 (or 62+2 GigE)
MDS 9506	4	2	192
MDS 9509	7	2	336
MDS 9513	13	11	528

Note: Throughout this chapter the term switch is used interchangeably for both Cisco MDS switches and directors.

4.1.8 Operating system

SAN-OS is the common operating system for all switches in the Cisco MDS9000 SAN switch family. Each switch is shipped with the latest Cisco MDS SAN-OS which consists of a kickstart and a system image.

To understand the concept of kickstart and system images, we briefly explain the boot sequence for a MDS 9000 family switch shown in Figure 4-1.

1. The BIOS performs HW component tests and loads the Loader.
2. The loader loads the kickstart image into RAM and starts the kickstart image.
3. The kickstart image loads the system image and starts the system image.
4. The system image reads the startup configuration file. When the system image has loaded you can access and manage the switch using the management interfaces.

We show this sequence in Figure 4-1.

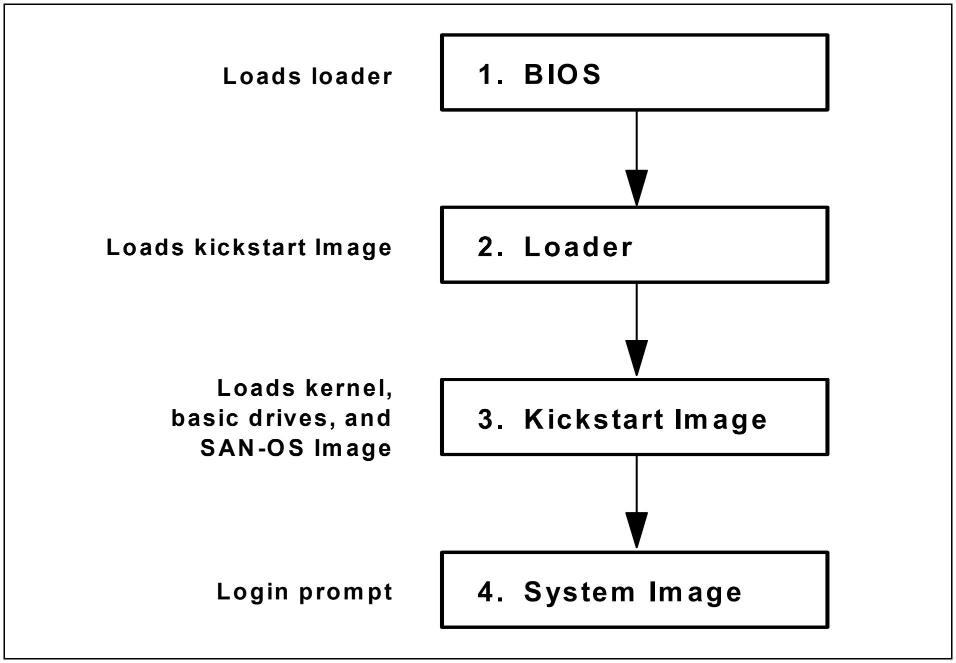

Loads loader
1. BIOS
Loads kickstart Image
2. Loader
Loads kernel, basic drives, and SAN-OS Image
3. Kickstart Image
Login prompt
4. System Image

Figure 4-1 Regular boot sequence

The kickstart and system image must be available for the switch to boot, and therefore it is placed in the bootflash. It is possible to boot from an external kickstart image placed on a TFTP server, although this requires manual intervention. This is only used when recovering from corrupted boot images, and the process is to copy the kickstart and system image to the bootflash (after verifying that the switch can boot from the kickstart image on the TFTP server).

4.1.9 Management tools

For switch and fabric management of the Cisco MDS 9000 family, both a Command line interface (CLI) and a Graphical User Interface (GUI) are available. The CLI uses either Telnet, SSH or serial console while the GUI based Fabric Manager toolset use SNMP when accessing the switches.

Cisco Fabric Manager

Cisco Fabric Manager is a network management toolset, using SNMPv3 (SNMP version 1 and 2 is also supported) when communicating with the MDS 9000 family switches (and 3rd party switches), providing a GUI to manage and perform real-time monitoring.

The toolset consists of the following components:

- **Fabric Manager Server:** Cisco Fabric Manager Server is the server component of the toolset and must be started prior to using Fabric Manager. When launching the GUI for the first time, the Fabric Manager Server is installed as a service on Windows (daemon on Linux or Solaris).
- **Device Manager:** Device Manager is a switch embedded Java application which is installed (and updated automatically) by Java Web start. While the Device Manager is somewhat complimentary to the Fabric Manager, the difference is that with Device Manager you manage a single switch, whereas with Fabric Manager you can manage multiple switches.
- **Fabric Manager Client:** Fabric Manager Client is a switch embedded Java application which is installed (and updated automatically) by Java Web start. With Fabric Manager switch and fabric configurations are performed.
- **Performance Manager:** Performance Manager is used for historic network device statistics collection and graphical presentation (in a Web browser), presenting recent statistics in detail and older statistics in summary. Performance Manager is set up using a configuration wizard.

Cisco CLI

From the CLI interface we can perform fabric and switch management, while the CLI parser provides both command help and command completion. The keyboard sequence stores previously used commands in the buffer history. Performing ongoing fabric and switch management using the GUI is somewhat more intuitive, and most switch commands are available, though when it comes to troubleshooting, comparably the CLI is a more powerful interface.

Licensing

The licensing model for the Cisco MDS 9000 family consists of two options:

- Feature based licensing, which implies a per switch cost, for features that apply to the entire switch.
- Module based licensing for features which require a specific hardware module such as the IPS module.

The standard license package, which is included with every Cisco MDS 9000 family switch (base configuration) includes standard SAN software features, while some advanced features are add-on options bundled in the following license packages and must be acquired separately.

- Cisco Enterprise Package (ENTERPRISE_PKG):
  - This package mainly consists of two types of advanced features:
    - *Advanced Traffic engineering features*, which are:
      - Inter-VSAN routing (IVR)
      - Quality of Service QoS
      - Extended Credits
      - Fibre Channel Write Acceleration and SCSI Flow statistics at LUN level (only available on SSM an ASM)
    - *Enhanced Network Security Features*, which are:
      - Fibre Channel Security Protocol (FC-SP) providing switch to switch and switch to host authentication
      - Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP) which can be combined with RADIUS or TACACS+ for remote authentication.
      - Hardware enforced LUN zoning
      - Read only zones
      - Port Security, mapping a specific device to be the only one able to access the fabric on a given port.
      - VSAN Based Access Control
      - IPsec, available for both FCIP and iSCSI
  - The license is acquired on a per switch basis, though some features require that all switches in the fabric have the license package.
- SAN Extension over IP Package (SAN_EXTN_OVER_IP):
  - This package enables integrated Fibre Channel Interface Protocol (FCIP) and must be acquired on a per module basis. IVR for FCIP is also included with this license.
- Cisco Mainframe Package (MAINFRAME_PKG):
  - This package enables IBM Fibre Connection (FICON) support and must be acquired on a per switch basis.
- Cisco Fabric Manager Server Package (FMSERVER_PKG):
  - This package extends the standard Cisco Fabric Manager toolset, providing historical performance monitoring, centralized management services and advanced application integration. This package is acquired on a per switch basis.
- Cisco MDS9000 Storage Service Enabler Package:
  - This package is currently not sold by IBM and is not discussed further.

Note: For a complete list of features within each license package, see the respective license package fact sheets:

http://www.cisco.com/en/US/products/hw/ps4159/ps4358/products_data_sheets_list.html

When buying the Cisco MDS 9000 family switch from IBM, the standard license package is always included. To see which other licenses are available with a specific switch type, refer to Table 4-2.

Table 4-2 Cisco MDS 9000 family licensing options

Switch model	ENTERPRISE	SAN_EXTN_OVER_IP	FMSERVER	MAINFRAME
MDS 9020	optional	NA	optional	NA
MDS 9120	optional	NA	optional	NA
MDS 9140	optional	NA	optional	NA
MDS 9216 (A/i)	optional	optional for 9216a	optional	optional
MDS 9506	optional	optional	optional	optional
MDS 9509	optional	optional	optional	optional

Security

Cisco’s SAN security suite provides secure SAN management access, which can be defined per VSAN offering customizable and granular Role Based Access Control (RBAC). This includes secure management protocols: SSH, SFTP, and SNMPv3; as well as switch-to-switch and host to switch authentication (FC-SP and DH-CHAP) and full RADIUS and TACACS+ accounting support.

For data access security, zoning can be defined based on WWN, port, LUN-zoning, read-only, and port-switch binding features.

For iSCSI hosts, CHAP authentication is supported.

4.2 Hardware

In this section we discuss several aspects of the hardware.

4.2.1 Port addressing and port modes

The Fibre Channel ports in the Cisco MDS 9000 family are numbered with addresses in the form of fc<slot>/<port>, where <slot> is the slot number of the line card (1-9), and <port> is the port number on the line card (1-32). For example, the first port of the line card in slot 1 is fc1/1, and the seventh port of the line card in slot 3 is fc3/7.

Fibre Channel IDs and persistent FCIDs

Contrary to other switch manufacturers, with the Cisco MDS 9000 family there is no fixed correlation between physical Fibre Channel ports and Fibre Channel IDs (FCID). This is necessary to allow intermixing line cards with different numbers of ports, while being able to utilize all port addresses, to allow both fabric and loop devices to coexist, and also to allow switches larger than 256 ports.

The primary reason for persistent FCIDs is to enable customers to move devices within a switch without having to rebind disk. This could be used in the case of a linecard or SFP failure, for example.

The following considerations apply to the FCID assignment for any VSAN:

- When an N_Port or NL_Port logs into the switch, it is assigned an FCID.
- N_Ports receive the same FCID if disconnected and reconnected to any port within the same switch, and within the same VSAN.
- NL_Ports receive the same FCID only if reconnected to the same port within the same switch where the port was originally connected.

If the persistent FCIDs feature is not enabled for a VSAN, the following considerations apply:

- The WWN of the N_Port or NL_Port and the assigned FCID are stored in a volatile cache, and are not saved across switch reboots.
- The switch preserves the binding of FCID to WWN on a best-effort basis.
- The volatile cache has room for a maximum of 4000 entries, and if the cache gets full, the oldest entries are overwritten.

If the persistent FCID feature is enabled for a VSAN, the following considerations apply:

- The FCID to WWN mapping of the WWNs currently in use is stored to a nonvolatile database, and is saved across reboots.
- The FCID to WWN mapping of any new device connected to the switch is automatically stored into the non-volatile database.
- You can also manually configure the FCID to WWN mappings if necessary.

Note: If you attach AIX or HP-UX hosts to a VSAN, you must have persistent FCIDs enabled for that VSAN. This is because these operating systems use the FCIDs in device addressing. If the FCID of a device changes, the operating system considers it to be a new device, and gives it a new name.

In general, we recommend enabling persistent FCIDs for your VSANs unless you have specific requirements that do not comply with persistent FCIDs.

Port modes

The Fibre Channel ports in the Cisco MDS 9000 family can operate in several modes. The operational modes are described in Table 4-3.

Table 4-3 Fibre Channel port operational modes

Mode	Description
E_Port	An expansion port (E_Port) interconnects two Fibre Channel switches, forming an ISL between an E_Port in each switch. The ISL belongs to a single VSAN, and can also be connected to third-party switches.
F_Port	A fabric port (F_Port) connects the switch to a N_Port in a host or storage device using a point-to-point link. Only one N_Port can connect to the F_Port.
FL_Port	A fabric loop port (FL_Port) connects the switch to a public FC-AL loop. Only one FL_Port can be operational in a single FC-AL loop at any given time.
TE_Port	A trunking E_Port (TE_Port) interconnects two Fibre Channel switches, forming an extended ISL (EISL) between a TE_Port in each switch. The EISL can multiplex the traffic of several VSANs. The EISL is currently only available in the Cisco MDS 9000 family of switches.
TL_Port	A translative loop port (TL_Port) connects the switch to a private FC-AL loop.
SD_Port	A SPAN destination port (SD_Port) acts as a snooper port, allowing the monitoring of the switch traffic with a standard Fibre Channel analyzer.
B_Port	A bridge port (B_Port) is used to connect some SAN extender devices to the switch, instead of E_Port.
Fx_Port	A Fx_Port can operate as either F_Port or FL_Port, depending on the device connected to it. The port mode is determined during interface initialization.

Mode	Description
Auto	A port configured as auto can operate as E_Port, F_Port, FL_Port, or TE_Port, depending on the device connected to it. The port mode is determined during interface initialization.

4.3 Operating system

Each switch is shipped with the latest Cisco MDS SAN-OS, which consists of a kickstart and a system image. Though the images are model specific the SAN-OS features are common across all platforms.

We recommend that you back up the running and startup configurations (if not the same) and system image on a regular basis. You can back up the configuration to the bootflash or to a remote server using either TFP, FTP, SCP, or SFTP.

Backing up the switch configuration using the CLI

If for some reason you have not saved the running configuration to the startup configuration we recommend to backup both the running and the startup config.

To back up the configuration using the CLI, we use the commands

```
copy running-config
copy startup-config
```

In Example 4-1 we use the commands to back up the running and the startup configuration to the bootflash and to an ftp-server, respectively.

Example 4-1 Backup the switch configuration

```
sc9509b# copy running-config bootflash:MDS1_Dec01_2005
sc9509b# dir bootflash:
       5449     Dec 01 06:12:33 2005  MDS1_Dec01_2005
--truncated--

sc9509b# copy nvram:startup-config
ftp://9.42.166.193/teams/sc/snapshot_MDS1_Dec012005
Enter username: ftp_user
Password:passphrase

-on the ftp server-
ftp> dir
-rw-------    1 14       50          5326 Dec 01 06:14 snapshot_MDS1_Dec012005
--truncated--
```

4.3.1 Upgrading the SAN-OS

In the topics that follow we describe how to upgrade the SAN-OS.

Note: We recommend that you always contact your IBM services representative prior to performing a SAN-OS upgrade, to review your software requirements based on your operating environment.

4.3.2 Upgrade prerequisites

When upgrading the SAN-OS on a Cisco MDS 9000 family switch, you must specify the variables that direct the switch to the images (kickstart and/or system).

Verify the following prerequisites prior to upgrading the software images:

- **Scheduling:** Verify that the fabric is stable and steady, while assuring that no switch or network configurations are performed when you plan to upgrade the switch, since all configurations are disallowed while the upgrade is running.
- **Space:** Verify that there is enough space available where you intend to copy the new software images to, this being the active and the standby supervisor bootflash.
- **Hardware:** Ensure that the switch is connected to a stable power source, since loss of power during the upgrade would potentially corrupt the image.
- **Connectivity:** Verify that you have connectivity to the server from which you are downloading the software images.
- **Images:** Verify that the specified system and kickstart images are compatible; if no kickstart image is specified, the running kickstart image is used. If a different system image is specified, you must verify that it is compatible with the running kickstart image.

When upgrading the SAN-OS on any Cisco MDS 9000 family switch running in production, we strongly recommend that you use the **`install all`** command, which provides a non-disruptive upgrade process.

Note: If you issue the **`install all`** command on a switch that only has a single supervisor system with kickstart and system image changes, or on a dual supervisor system with incompatible system software images, then the process is disruptive!

Any upgrades to a Caching Services module (CSM) or IP Storage services module (IPS) are disruptive for that module.

For switches **not** running in production, you can alternatively do the quick upgrade procedure using the **`reload`** command; this process is disruptive.

Install all

Using the **`install all`** command provides you the ability to upgrade a switch in the least disruptive way. When invoked, the command first checks the image integrity, including the running kickstart and system images, and performs a platform validity check of the image you are upgrading to. When the validation is performed, you are presented with an overview of the changes (and impact), and you are prompted to confirm the upgrade process to start (or cancel).

Quick upgrade

Performing a quick upgrade using the **`reload`** command is ***only*** recommended for switches not in production while on completion the switch is rebooted. The process is to copy the kickstart and system image to the switch, set the boot variables, and issue the **`reload`** command; when completed, the switch is rebooted.

Manual upgrade

Performing a manual installation is only recommended for experienced administrators who are completely familiar with switch configurations. For further detail on how to perform manual upgrades, consult the *Cisco MDS 9000 family Configuration Guide*:

`http://www.cisco.com/en/US/products/ps5989/products_installation_and_configuration_guides_list.html`

4.4 Management Tools

For switch and fabric management of the Cisco MDS 9000 family, both a Command Line Interface (CLI) and a Graphical User Interface (GUI) is available. The CLI uses either Telnet, SSH, or serial console, while the GUI based Fabric Manager toolset use SNMP when accessing the switches.

Cisco Fabric Manager and Cisco Device Manager software is embedded in every Cisco MDS 9000 family Switch. This software is downloaded and installed automatically through Java Web Start when you access a switch via a supported, Java-enabled Web browser, such as Windows Internet Explorer, or Netscape Navigator.

In the following sections, all examples are performed on a management console running Windows.

4.4.1 Launching the CLI

Apart from invoking the CLI from the GUI interfaces, we can connect to the switch using either Telnet, SSH, or a serial connection physically connected to the switch. In Example 4-2 we connect to the switch via Telnet.

Example 4-2 Connecting via Telnet

```
c:\Telnet 9.42.164.80

sc9509b login: marcus
Password:
Cisco Storage Area Networking Operating System (SAN-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2004, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.
sc9509b#
```

Using the CLI provides you with the possibility to perform management tasks using scripts which access the switch utilizing the CLI.

CLI command Modes

The Cisco MDS 9000 family CLI has two main command modes, the user EXEC mode and the configuration mode. The commands available to you depend on the mode you are in. To obtain a list of available commands in either mode, type a question mark (?) at the system prompt.

Exec Mode

The EXEC mode is used to display system information, perform basic tests, and perform basic system operations. Changes made in EXEC mode are generally not saved across system resets (not saved to the startup config).

By default you enter the user EXEC mode when logging on to a switch using the CLI; when in EXEC mode, the prompt is *SwitchName#*.

Configuration mode

The configuration mode enables you to configure features that affect the system as a whole. Changes made in this mode are saved across system resets if you save your configuration (save to startup configuration).

To enter the config mode when in EXEC mode, we enter the command **`config terminal`** and the prompt changes to *SwitchName(config)#*.

To return to EXEC mode when in config mode, use the command **`end`**, or press <Ctrl-z>.

Tip: You can abbreviate commands and keywords by entering just enough characters to make the command unique from other commands. For example, you can abbreviate the config terminal command to **`conf t`**.

Note: The Cisco MDS 9000 family CLI command structure is very similar to that of the Cisco IOS (Internetwork Operating System) commands.

4.4.2 System requirements for GUI management tools

We verify that the hardware and software requirements are met for the Cisco Fabric Manager clients and servers as listed below (for the latest requirements, see the release notes):

Processor

- Intel Pentium III 500 MHz processor (minimum) for Windows and Linux
- Sun UltraSPARC 550 MHz processor (minimum) for Solaris

Memory

- 128 MB (minimum)

Disk space

- Cisco Fabric Manager application - 6 MB
- Java Virtual Machine - 35 MB
- Historical performance statistics - 76 KB per port or flow monitored

Software

- Windows 2000 or XP, Solaris 2.8, Red Hat Linux operating systems
- Java Virtual Machine version 1.4 or later (version 1.4.2 is recommended minimum level to support current Fabric Manager and Device Manager)
- TCP/IP software stack

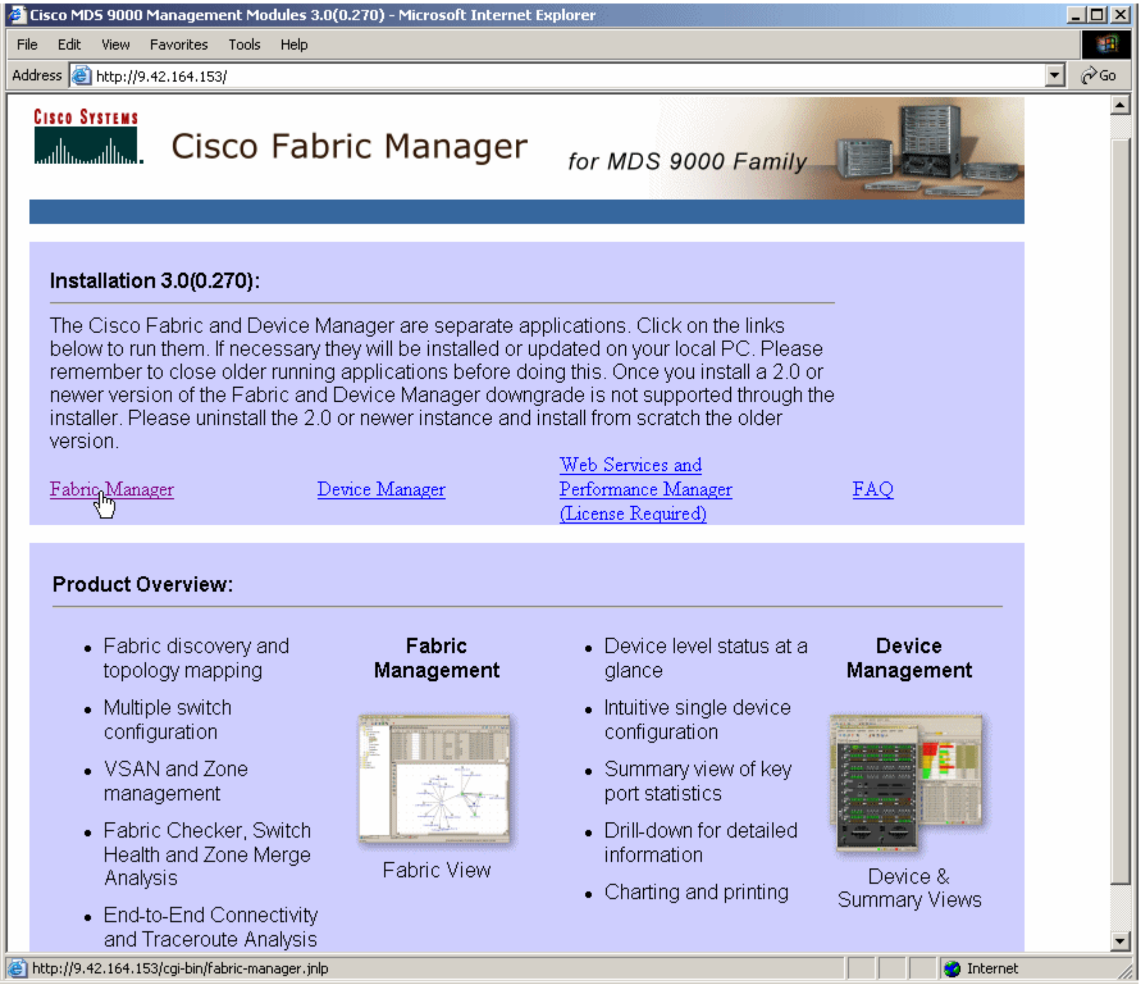
Protocols

Cisco Fabric Manager uses these standard protocols:

- SNMP Versions 1, 2c, and 3
- HTTP

4.4.3 Launching Fabric Manager

To launch Fabric Manager, we use a Web browser and point to the IP address of the switch we want to manage. When presented with the Cisco Fabric Manager GUI frontpage, we select **Fabric Manager**, as shown in Figure 4-2.


Cisco MDS 9000 Management Modules 3.0(0.270) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://9.42.164.153/
Go
Cisco Systems
Cisco Fabric Manager
for MDS 9000 Family

Installation 3.0(0.270):

The Cisco Fabric and Device Manager are separate applications. Click on the links below to run them. If necessary they will be installed or updated on your local PC. Please remember to close older running applications before doing this. Once you install a 2.0 or newer version of the Fabric and Device Manager downgrade is not supported through the installer. Please uninstall the 2.0 or newer instance and install from scratch the older version.

Fabric Manager | Device Manager | Web Services and Performance Manager (License Required) | FAQ

Product Overview:

Fabric Management

- Fabric discovery and topology mapping
- Multiple switch configuration
- VSAN and Zone management
- Fabric Checker, Switch Health and Zone Merge Analysis
- End-to-End Connectivity and Traceroute Analysis

Fabric View

Device Management

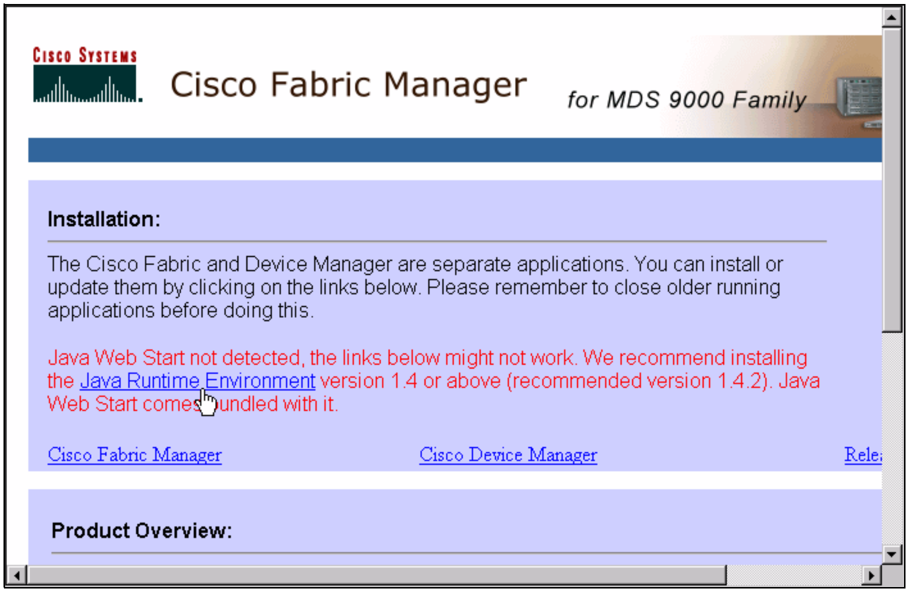
- Device level status at a glance
- Intuitive single device configuration
- Summary view of key port statistics
- Drill-down for detailed information
- Charting and printing

Device & Summary Views

http://9.42.164.153/cgi-bin/fabric-manager.jnlp
Internet

Figure 4-2 Launching Fabric Manager

If you get any error messages at this point, you might not have the prerequisite software installed. For example, if you do not have *Java Web Start* installed, you get an error message similar to that shown in Figure 4-3, and you must install the required Java, after which you can relaunch Fabric Manager.



Installation:

The Cisco Fabric and Device Manager are separate applications. You can install or update them by clicking on the links below. Please remember to close older running applications before doing this.

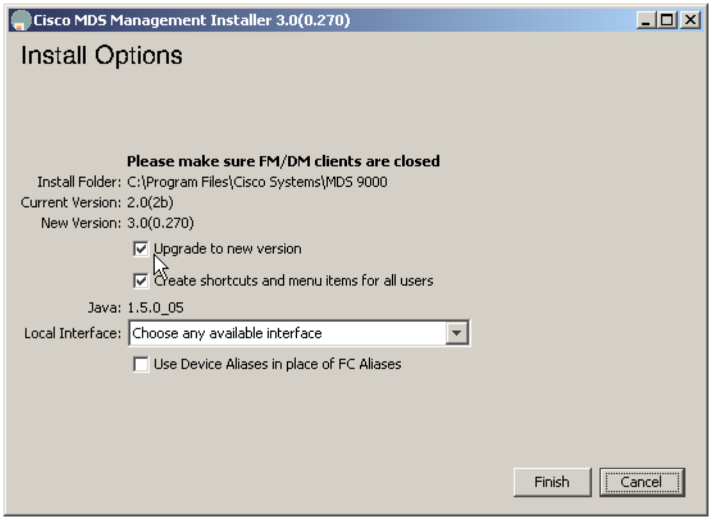
Java Web Start not detected, the links below might not work. We recommend installing the Java Runtime Environment version 1.4 or above (recommended version 1.4.2). Java Web Start comes bundled with it.

Product Overview:

Figure 4-3 Java Web Start not detected

The java Web Start launches and we are presented with the install options as shown next in Figure 4-4. We choose to upgrade the Fabric Manager. Since we have upgraded our director to SAN-OS 3.x and new binaries are available, we are also prompted regarding which ethernet interface to use and whether we want to use Global Device Aliases.

> **Note:** If this is the first time you are launching Fabric Manager, you are also prompted regarding where to place the binaries for Fabric Manager and inquiring whether shortcuts should be placed on the desktop. Subsequently the Cisco MDS Database Server and Cisco MDS Fabric Manager services are installed and Fabric Manager is started.


Cisco MDS Management Installer 3.0(0.270)
Install Options

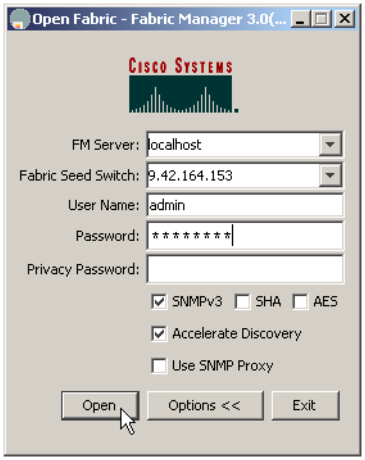
Please make sure FM/DM clients are closed

Install Folder: C:\Program Files\Cisco Systems\MDS 9000
Current Version: 2.0(2b)
New Version: 3.0(0.270)
☑ Upgrade to new version
☑ Create shortcuts and menu items for all users
Java: 1.5.0_05
Local Interface: Choose any available interface
☐ Use Device Aliases in place of FC Aliases

Finish
Cancel

Figure 4-4 Cisco MDS Management installer options

The Fabric Manager upgrade completes and we enter our login credentials to authenticate and connection properties, as shown in Figure 4-5.

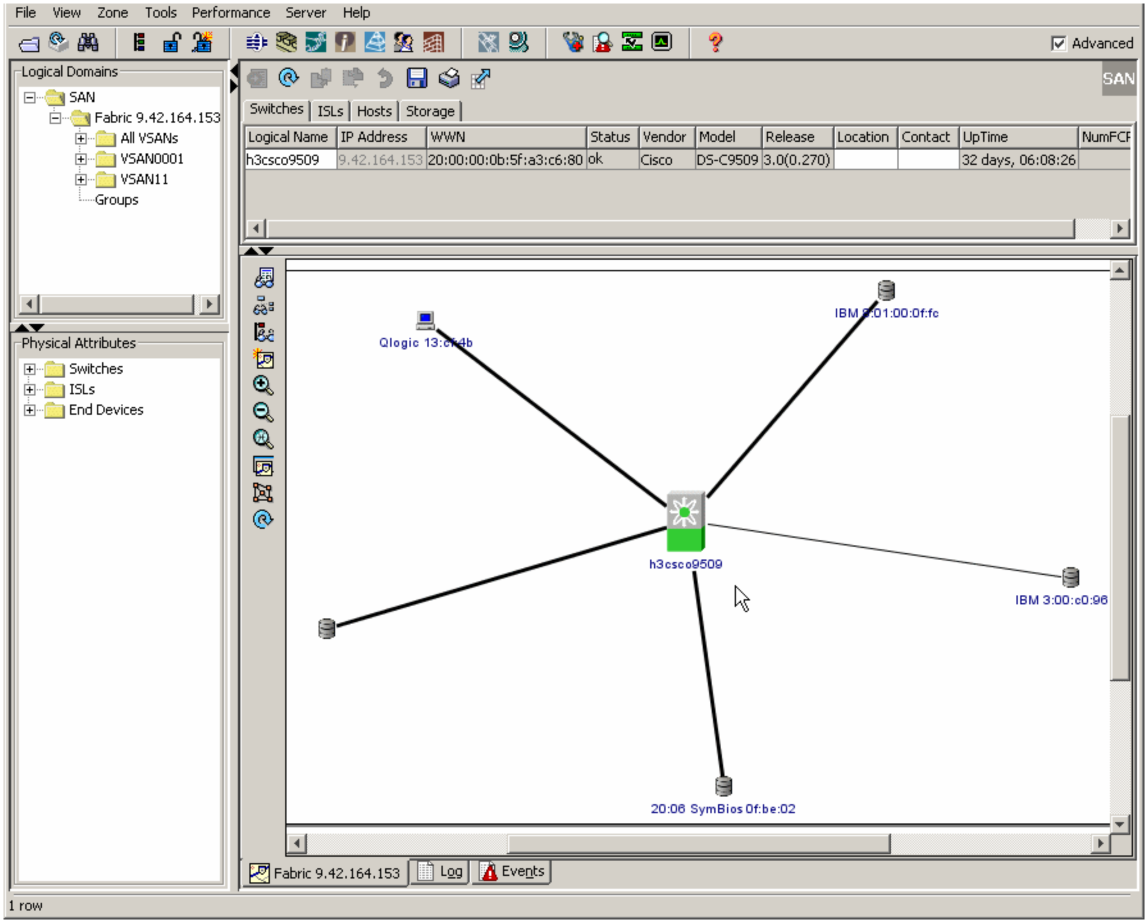

Open Fabric - Fabric Manager 3.0(...
Cisco Systems

FM Server: localhost
Fabric Seed Switch: 9.42.164.153
User Name: admin
Password: ********
Privacy Password:
☑ SNMPv3 ☐ SHA ☐ AES
☑ Accelerate Discovery
☐ Use SNMP Proxy

Open
Options <<
Exit

Figure 4-5 Login to FM server

The Fabric Manager is started and we are presented with a logical view of the switch fabric as shown in Figure 4-6.


File
View
Zone
Tools
Performance
Server
Help
☑ Advanced
SAN
Logical Domains
SAN
Fabric 9.42.164.153
All VSANs
VSAN0001
VSAN11
Groups
Physical Attributes
Switches
ISLs
End Devices
Switches
ISLs
Hosts
Storage
Qlogic 13:cf:4b
IBM 8:01:00:0f:fc
h3csco9509
IBM 3:00:c0:96
20:06 SymBios 0f:be:02
Fabric 9.42.164.153
Log
Events
1 row

Logical Name	IP Address	WWN	Status	Vendor	Model	Release	Location	Contact	UpTime	NumFCF
h3csco9509	9.42.164.153	20:00:00:0b:5f:a3:c6:80	ok	Cisco	DS-C9509	3.0(0.270)			32 days, 06:08:26	

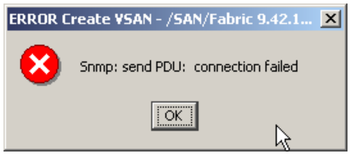
Figure 4-6 Fabric Manager logical view

The Fabric Manager windows shows a graphical presentation of our switch fabric on the bottom right, an information area on the top, a navigation window on the left, which is divided into a logical menu at the top and a physical menu at the bottom. The content of the information area changes accordingly to represent the selection chosen in the navigation menu, showing the current selection at the top of the information area.

SNMP time-outs

The Fabric Manager uses the SNMP protocol to communicate with the switch. SNMP is a stateless protocol, and when you apply changes to the switch, the Fabric Manager sends a request packet with the changes to the switch and waits for a response packet.

Depending on your network, either the request packet or the response packet might end up being dropped. This results in a SNMP time-out message, similar to that shown in Figure 4-7.

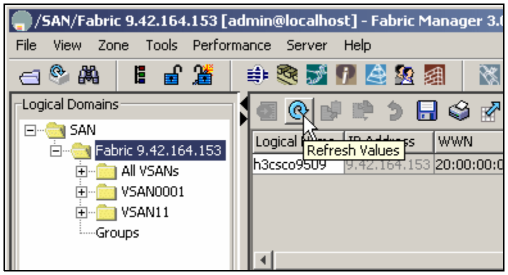


ERROR Create VSAN - /SAN/Fabric 9.42.1...

Snmp: send PDU: connection failed

Figure 4-7 SNMP connection failed

If you get this message, you do not know which of the packets was dropped. This means that you do not know if your changes are applied to the switch or not. We recommend that you click the **Refresh Values** button as shown in Figure 4-8 to ensure that the information in the Fabric Manager is up to date before making any further changes.

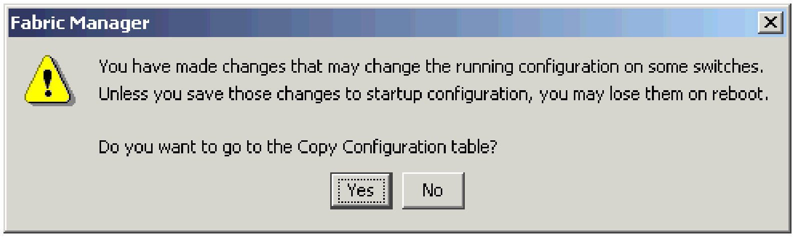


/SAN/Fabric 9.42.164.153 [admin@localhost] - Fabric Manager 3.(
File View Zone Tools Performance Server Help
Logical Domains
SAN
Fabric 9.42.164.153
All VSANs
VSAN0001
VSAN11
Groups
Refresh Values
Logical
IP Address
WWN
h3csco9509
9.42.164.153
20:00:00:0

Figure 4-8 Refresh displayed values

Stopping Fabric Manager

If you have made changes to the Cisco running configuration that have not yet been copied to the startup configuration, you get a message similar to that shown in Figure 4-9 when you exit from, or leave an FM session.



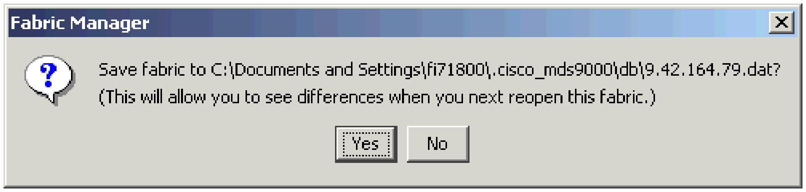
You have made changes that may change the running configuration on some switches. Unless you save those changes to startup configuration, you may lose them on reboot.

Do you want to go to the Copy Configuration table?

Figure 4-9 Unsaved running configuration warning

You can click **Yes** to go to the Copy Configuration window, and then click **Apply Changes** to do the actual copy, and wait for the copy processes to finish. After all of the copy processes are finished you can close the Fabric Manager.

The Fabric Manager can also save information about your switch fabric into a local database in your workstation. If you have changes that have not been saved, you get a message similar to that shown in Figure 4-10.



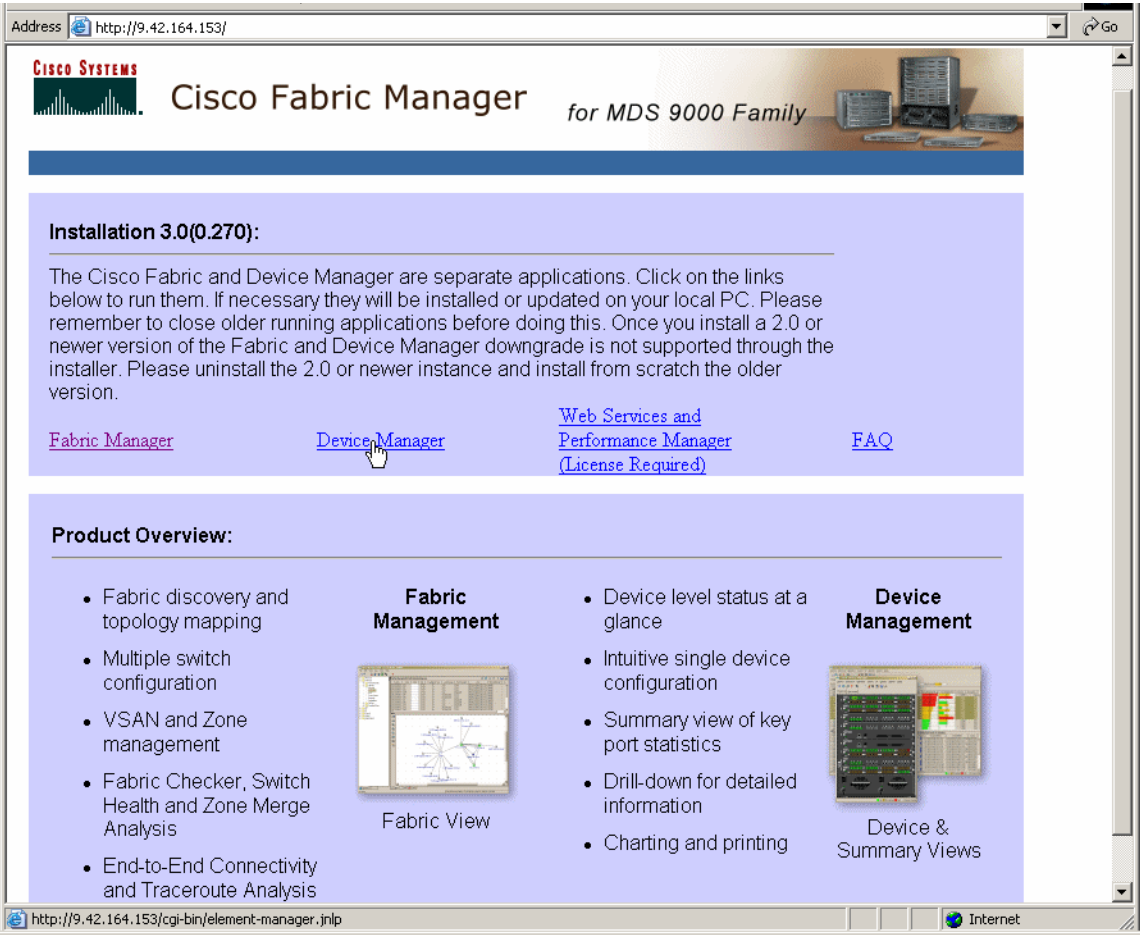
Save fabric to C:\Documents and Settings\fi71800\.cisco_mds9000\db\9.42.164.79.dat?
(This will allow you to see differences when you next reopen this fabric.)

Figure 4-10 Unsaved local fabric database warning

Since having the local database up to date helps you to see any changes to the fabric, when you open the Fabric Manager again, it is a good idea to click **Yes** here.

4.4.4 Launching Device Manager

To launch Device Manager, we use a Web browser and point to the IP address of the switch we want to manage. When we click **Device Manager** as shown in Figure 4-11, the Device Manager is installed.


Address
http://9.42.164.153/
Go
Cisco Systems
Cisco Fabric Manager
for MDS 9000 Family

Installation 3.0(0.270):

The Cisco Fabric and Device Manager are separate applications. Click on the links below to run them. If necessary they will be installed or updated on your local PC. Please remember to close older running applications before doing this. Once you install a 2.0 or newer version of the Fabric and Device Manager downgrade is not supported through the installer. Please uninstall the 2.0 or newer instance and install from scratch the older version.

Fabric Manager
Device Manager
Web Services and Performance Manager (License Required)
FAQ

Product Overview:

Fabric Management

- Fabric discovery and topology mapping
- Multiple switch configuration
- VSAN and Zone management
- Fabric Checker, Switch Health and Zone Merge Analysis
- End-to-End Connectivity and Traceroute Analysis

Fabric View

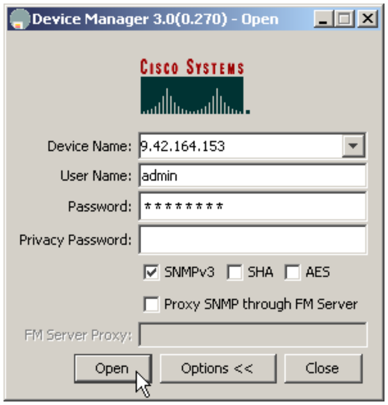
Device Management

- Device level status at a glance
- Intuitive single device configuration
- Summary view of key port statistics
- Drill-down for detailed information
- Charting and printing

Device & Summary Views
http://9.42.164.153/cgi-bin/element-manager.jnlp
Internet

Figure 4-11 Launching Device Manager for the first time

When the Device Manager has initialized, we are prompted for authentication to login to the switch, and we use the same user name and password as for Fabric Manager shown in Figure 4-12.


Device Manager 3.0(0.270) - Open
Cisco Systems
Open
Options <<
Close

Device Name: 9.42.164.153
User Name: admin
Password: ********
Privacy Password:
☑ SNMPv3 ☐ SHA ☐ AES
☐ Proxy SNMP through FM Server
FM Server Proxy:

Figure 4-12 Device Manager login

Upon successful login, the Device Manager application is started and we are presented with a graphical representation of the physical switch as shown in Figure 4-13.

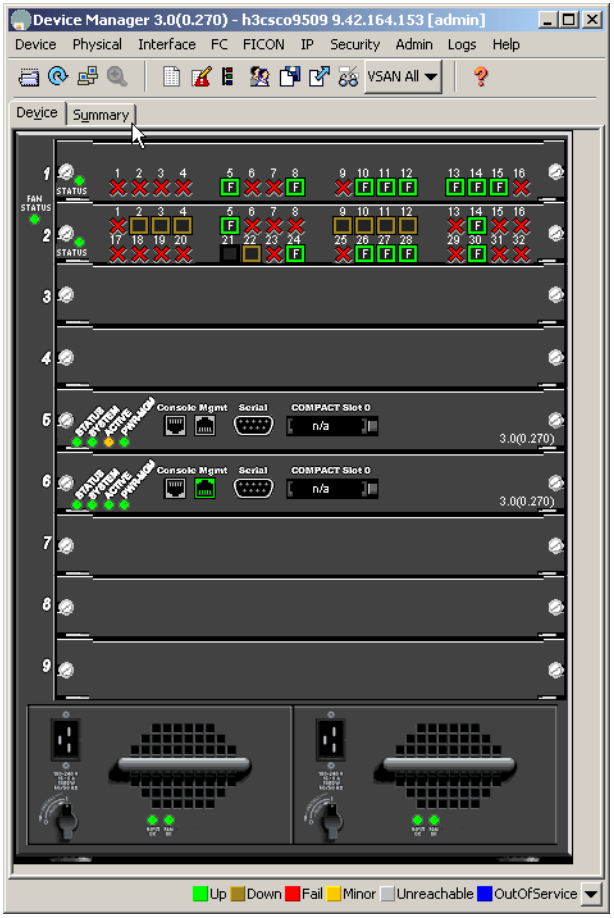
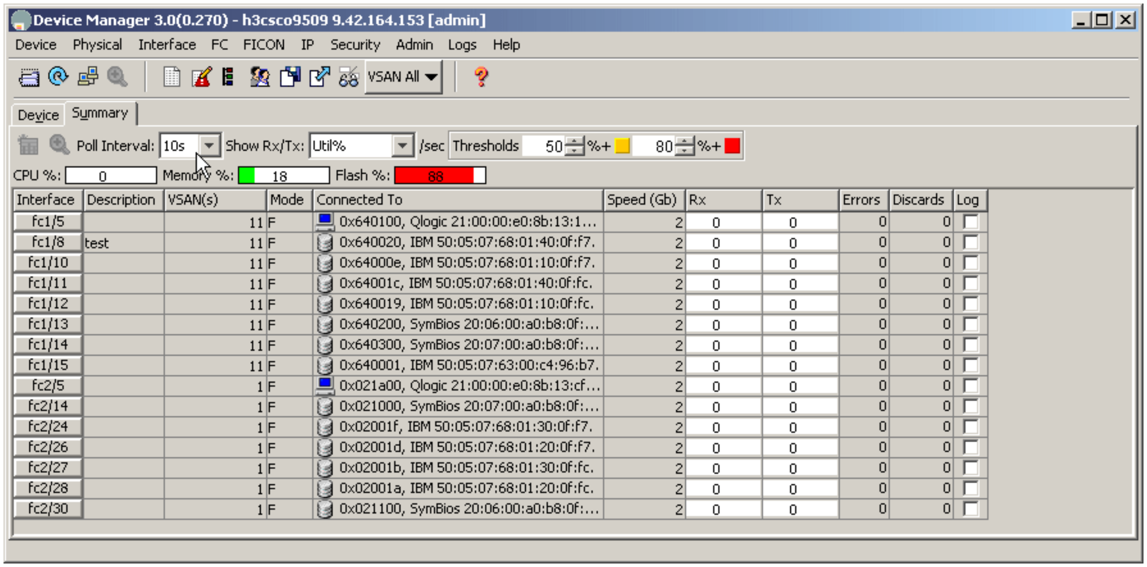

Device Manager 3.0(0.270) - h3csco9509 9.42.164.153 [admin]
Device
Physical
Interface
FC
FICON
IP
Security
Admin
Logs
Help
VSAN All
Device
Summary
FAN STATUS
STATUS
Console Mgmt
Serial
COMPACT Slot 0
n/a
3.0(0.270)
Up
Down
Fail
Minor
Unreachable
OutOfService

Figure 4-13 Device Manager

The Device Manager window shows a graphical presentation of our switch displaying the power and fan trays and the switch modules and respective ports installed.

To display a summary of the switch, we click the **Summary** tab, shown in Figure 4-14, displaying an overview of the utilization of the switch.


Device Manager 3.0(0.270) - h3csco9509 9.42.164.153 [admin]
Device Physical Interface FC FICON IP Security Admin Logs Help
VSAN All
Device
Summary

Poll Interval: 10s Show Rx/Tx: Util% /sec Thresholds 50 %+ 🟨 80 %+ 🟥

CPU %: 0 Memory %: 18 Flash %: 88

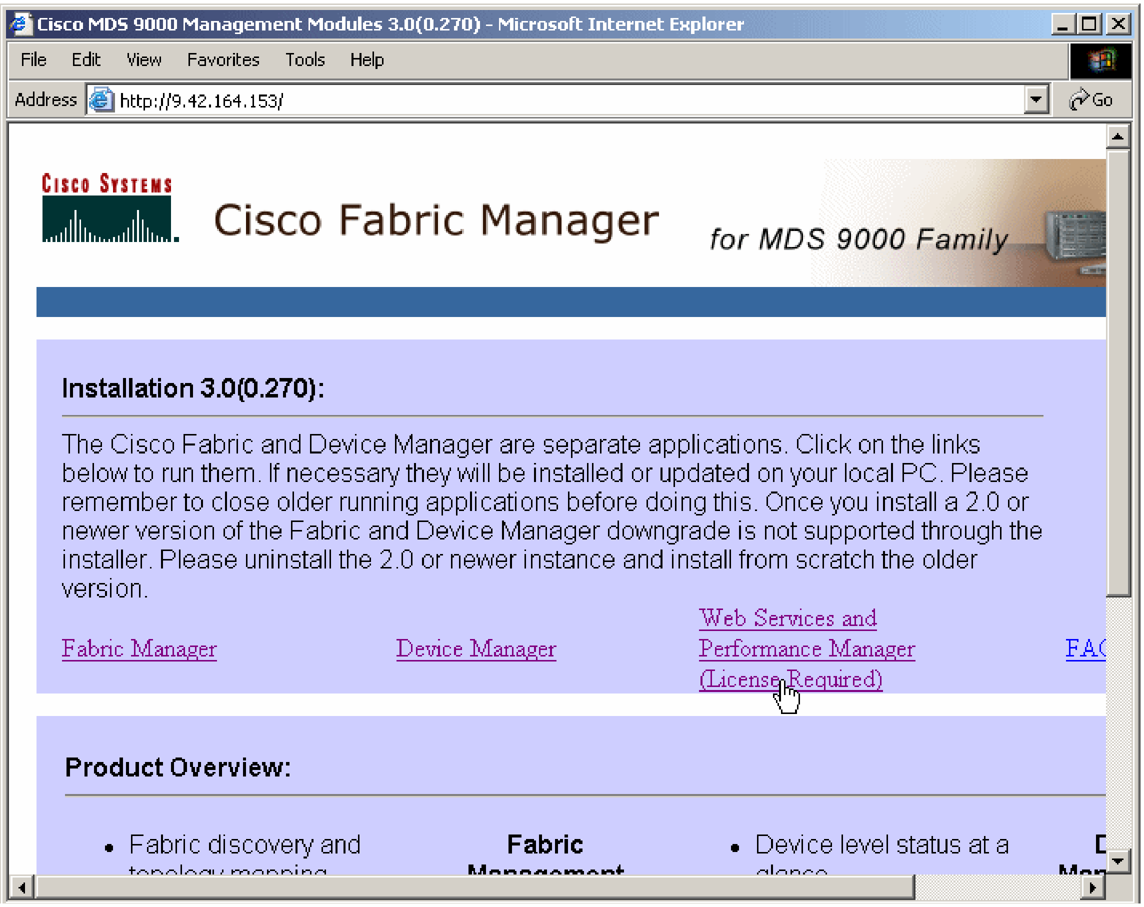
Interface	Description	VSAN(s)	Mode	Connected To	Speed (Gb)	Rx	Tx	Errors	Discards	Log
fc1/5		11	F	0x640100, Qlogic 21:00:00:e0:8b:13:1...	2	0	0	0	0	☐
fc1/8	test	11	F	0x640020, IBM 50:05:07:68:01:40:0f:f7.	2	0	0	0	0	☐
fc1/10		11	F	0x64000e, IBM 50:05:07:68:01:10:0f:f7.	2	0	0	0	0	☐
fc1/11		11	F	0x64001c, IBM 50:05:07:68:01:40:0f:fc.	2	0	0	0	0	☐
fc1/12		11	F	0x640019, IBM 50:05:07:68:01:10:0f:fc.	2	0	0	0	0	☐
fc1/13		11	F	0x640200, SymBios 20:06:00:a0:b8:0f:...	2	0	0	0	0	☐
fc1/14		11	F	0x640300, SymBios 20:07:00:a0:b8:0f:...	2	0	0	0	0	☐
fc1/15		11	F	0x640001, IBM 50:05:07:63:00:c4:96:b7.	2	0	0	0	0	☐
fc2/5		1	F	0x021a00, Qlogic 21:00:00:e0:8b:13:cf...	2	0	0	0	0	☐
fc2/14		1	F	0x021000, SymBios 20:07:00:a0:b8:0f:...	2	0	0	0	0	☐
fc2/24		1	F	0x02001f, IBM 50:05:07:68:01:30:0f:f7.	2	0	0	0	0	☐
fc2/26		1	F	0x02001d, IBM 50:05:07:68:01:20:0f:f7.	2	0	0	0	0	☐
fc2/27		1	F	0x02001b, IBM 50:05:07:68:01:30:0f:fc.	2	0	0	0	0	☐
fc2/28		1	F	0x02001a, IBM 50:05:07:68:01:20:0f:fc.	2	0	0	0	0	☐
fc2/30		1	F	0x021100, SymBios 20:06:00:a0:b8:0f:...	2	0	0	0	0	☐

Figure 4-14 Device Manager summary

4.4.5 Launching Performance Manager

To launch Performance Manager, we use a Web browser and point to the IP address of the switch we want to manage, shown in Figure 4-15.

> **Note:** To be able to use the Performance Manager, you must acquire and install the Cisco Fabric Manager Server Package (FMSERVER_PKG), if not already present on the switch.


Cisco MDS 9000 Management Modules 3.0(0.270) - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Address
http://9.42.164.153/
Go
Cisco Systems
Cisco Fabric Manager
for MDS 9000 Family

Installation 3.0(0.270):

The Cisco Fabric and Device Manager are separate applications. Click on the links below to run them. If necessary they will be installed or updated on your local PC. Please remember to close older running applications before doing this. Once you install a 2.0 or newer version of the Fabric and Device Manager downgrade is not supported through the installer. Please uninstall the 2.0 or newer instance and install from scratch the older version.

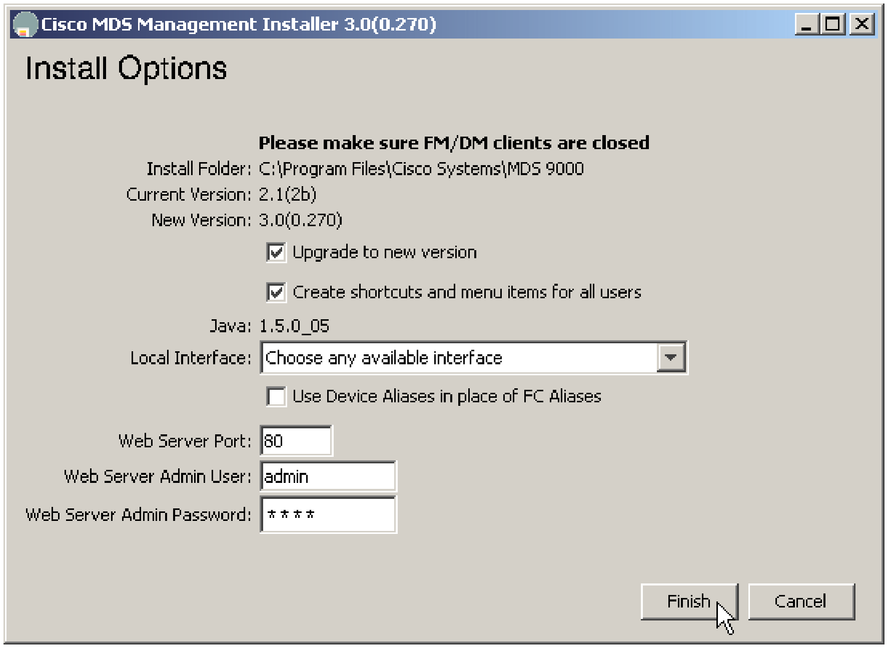
Fabric Manager
Device Manager
Web Services and Performance Manager (License Required)
FA

Product Overview:

Fabric discovery and
Fabric
Device level status at a

Figure 4-15 Launching Performance Manager

The Cisco MDS Management installer prompts for a Web server username and password as shown in Figure 4-16. We enter the login credentials, click **Finish**, and Performance manager is installed.



Please make sure FM/DM clients are closed

Install Folder: C:\Program Files\Cisco Systems\MDS 9000

Current Version: 2.1(2b)

New Version: 3.0(0.270)

☑ Upgrade to new version

☑ Create shortcuts and menu items for all users

Java: 1.5.0_05

Local Interface: Choose any available interface

☐ Use Device Aliases in place of FC Aliases

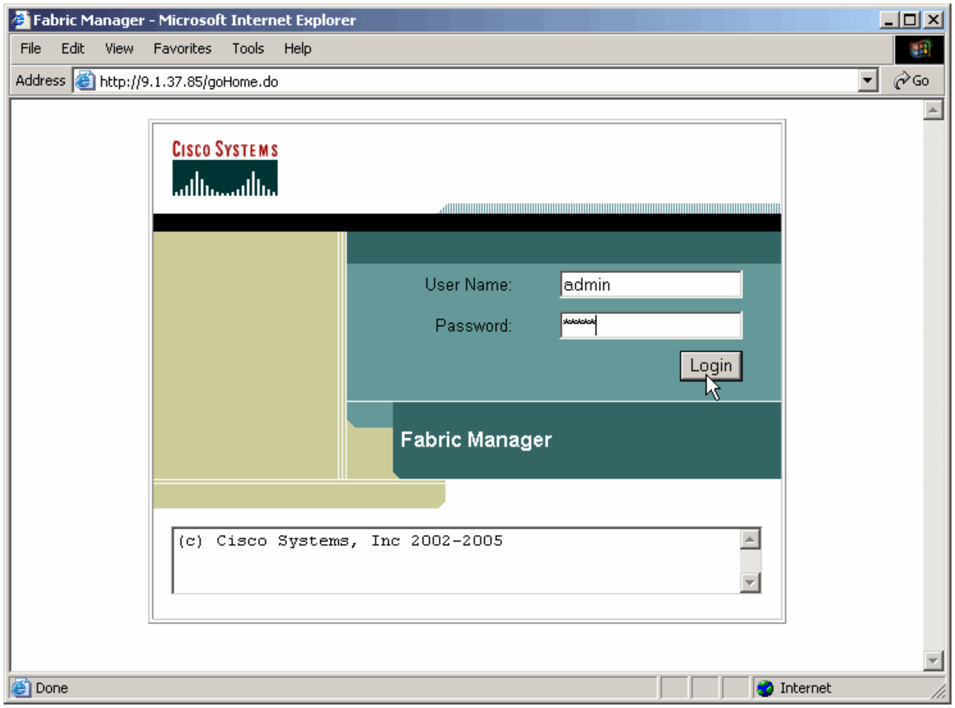
Web Server Port: 80

Web Server Admin User: admin

Web Server Admin Password: ****

Figure 4-16 Install options for Cisco Performance Manager (and Web Server)

The installation completes and we are presented with the Performance Manager login screen shown in Figure 4-17.


Fabric Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://9.1.37.85/goHome.do
Go
CISCO SYSTEMS
Login
Fabric Manager
Done
Internet

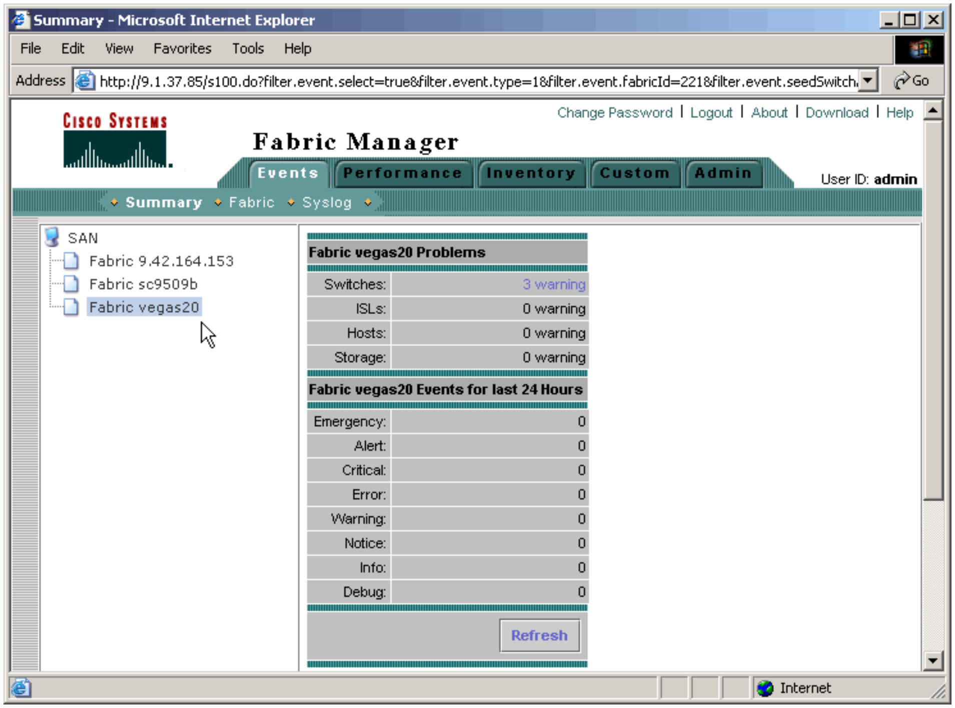
User Name: admin

Password: *****

(c) Cisco Systems, Inc 2002-2005

Figure 4-17 Login to Performance Manager

In Figure 4-18 we are presented with an overview of fabrics and events.


Summary - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Go
CISCO SYSTEMS
Change Password | Logout | About | Download | Help
Fabric Manager
Events
Performance
Inventory
Custom
Admin
User ID: admin
Summary
Fabric
Syslog
SAN
Fabric 9.42.164.153
Fabric sc9509b
Fabric vegas20
Refresh
Internet

Address: http://9.1.37.85/s100.do?filter.event.select=true&filter.event.type=1&filter.event.fabricId=221&filter.event.seedSwitch

Fabric vegas20 Problems	
Switches:	3 warning
ISLs:	0 warning
Hosts:	0 warning
Storage:	0 warning

Fabric vegas20 Events for last 24 Hours	
Emergency:	0
Alert:	0
Critical:	0
Error:	0
Warning:	0
Notice:	0
Info:	0
Debug:	0

Figure 4-18 Overview of fabrics and events

4.4.6 Obtaining the latest source files

Directors and switches in the Cisco MDS 9000 Multilayer Fabric Switch Family are shipped with the current levels of firmware already installed at the time of shipping. This code level is usually sufficient to begin the switch implementation process, but we recommend that you regularly check for the latest supported code levels and install updated code when required.

To check the currently supported levels of code for the Cisco MDS 9000 switch family, go to the following Web page and select the specific switch or director:

`http://www-03.ibm.com/servers/storage/support/san/index.html`

Attention: Cisco regularly makes new code releases available on their Web site for authorized users to download. IBM conducts additional integration testing on this code before issuing its approval, so we recommend that you always install only the IBM recommended code levels.

If you experience problems with an unapproved code release, IBM might ask you to install an approved release before continuing with problem resolution.

4.5 Security

The Cisco MDS 9000 family switches provides the following secure switch management options:

- Switch access security:
  - Secure Shell (SSH) can be enabled on each switch to ensure secure access using the CLI, providing encrypted user authentication and data exchange.
  - SNMPv3 is the default protocol for the GUI interfaces providing secure user authentication and data encryption.
  - IP access control list (IP-ACL) can be enabled to provide basic network security based on IP-ACL.
- User authentication:
  - User authentication can either be verified locally on each switch or remotely for all switches using either a (or more) TACACS+ or RADIUS server providing central use management.
  - Role based access control enables you to define the permissions associated with each user, as well as stretching permissions on a per VSAN level.
- Port security:
  - To prevent unauthorized switch port access, enable the switch port security feature which rejects device or switch logins, and any intrusion attempt are forwarded as a syslog message. Port security is defined on a specific world wide node name (WWN), world wide port name (WWPN) or a range of WWNs or WWPNs.
- Fabric security:
  - For enhanced fabric security Fibre Channel Security Protocol (FC-SP) can be enabled to provide encrypted authentication of and communication of switch-to-switch and HBA-to-switch communication based on Diffie Hellman Challenge Handshake Authentication Protocol (DH-CHAP) for verification.

Note: At the time of writing, the support for FC-SP for HBAs is limited, and their use in the industry so far is merely for switch-to-switch communication.

4.6 Implementation

In this section we go through the steps necessary to implement and set up the Cisco MDS 9000 family switches.

4.6.1 Initial setup of the Cisco MDS 9000 family

Before you can manage the Cisco MDS 9000 series switch through the network, you have to set up the TCP/IP parameters for the switch.

The first time the switch is powered on, it automatically runs the setup program, and prompts you for the IP address and other configuration information necessary to communicate over the management ethernet interface. You can also start the setup program with the **`setup`** command later if necessary.

4.6.2 Preparing to configure the switch

Before you configure the switch for the first time, you should gather the following information:

- New administrator password
- Switch name
- IP address for the management ethernet
- Subnet mask for the management ethernet
- Default gateway IP address (optional)
- DNS server IP address (optional)
- NTP server IP address (optional)
- SNMP v3 secret key (optional)

4.6.3 Connecting to the switch via the serial port

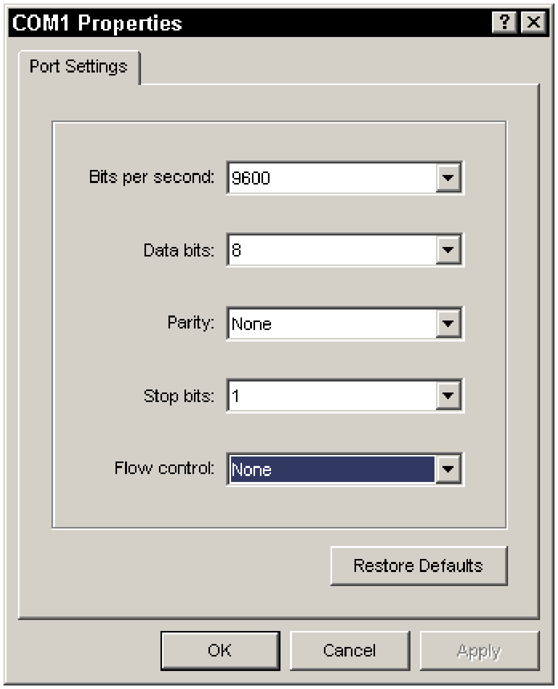
Here are the steps for this procedure:

1. Connect the serial cable provided with the switch to the RJ-45 socket in the switch, using the console port in these modules:
   - Interface module in MDS 9100 or 9200
   - Supervisor module in slot 5/6 in the MDS 9500 directors.
2. Connect the other end of the serial cable to an RS-232 serial port on the workstation.

3. Disable any serial communication programs running on the workstation.
4. Open a terminal emulation application (such as HyperTerminal on a PC), and configure it as follows:

   ```
   Bits per second: 9600
   Data bits: 8
   Parity: none
   Stop bits: 1
   Flow control: none
   ```

   An example of the HyperTerminal serial port properties window is shown in Figure 4-19.



Bits per second: 9600
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None

Figure 4-19 HyperTerminal serial port properties window

4.6.4 Setting up the initial parameters with the setup program

We assume you are already connected to the console serial port of the switch, but that the switch is still powered off. In Example 4-3 we connect to an MDS 9216 and power on the switch. The *Basic System Configuration Dialog* starts.

Note: The steps shown in our example might differ, depending on which features you want to activate and configure. However, the prompts in the *Basic System Configuration Dialog* are somewhat self-explanatory.

Example 4-3 Initial setup -powering up the switch

```
Enter the password for "admin":
Confirm the password for "admin":

      ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco MDS 9000 family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. MDS devices must be registered to receive entitled
support services.

Press Enter at anytime to skip a dialog.
Use ctrl-c at anytime to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes


  Create another login account (yes/no) [n]: no

 Configure read-only SNMP community string (yes/no) [n]: no

 Configure read-write SNMP community string (yes/no) [n]: no

  Enter the switch name : h3csco9509

Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: yes

    Mgmt0 IP address : 9.11.195.29

    Mgmt0 IP netmask : 255.255.255.0

 Configure the default gateway? (yes/no) [y]: yes

   IP address of the default gateway : 9.11.195.1

 Configure advanced IP options? (yes/no) [n]: yes

Continue with In-band (vsan1) management configuration? (yes/no) [n]: no

  Enable IP routing? (yes/no) [n]: no

  Configure static route? (yes/no) [n]: no

 Configure the default network? (yes/no) [n]: no
```

```
  Configure the DNS IP address? (yes/no) [n]: yes

    DNS IP address : 9.11.224.114

  Configure the default domain name? (yes/no) [n]: no

  Enable the telnet service? (yes/no) [y]: yes

  Enable the ssh service? (yes/no) [n]: no

  Configure the ntp server? (yes/no) [n]: no

  Configure default switchport interface state (shut/noshut) [shut]: noshut

  Configure default switchport trunk mode (on/off/auto) [on]: auto

  Configure default zone policy (permit/deny) [deny]:

  Enable full zoneset distribution? (yes/no) [n]:

The following configuration will be applied:
  switchname h3csco9509
  interface mgmt0
    ip address 9.11.195.29 255.255.255.0
    no shutdown
  ip default-gateway 9.11.195.1
  ip name-server 9.11.224.114
  telnet server enable
  no ssh server enable
  no system default switchport shutdown
  system default switchport trunk mode auto
  no zone default-zone permit vsan 1-4093
  no zoneset distribute full vsan 1-4093

Would you like to edit the configuration? (yes/no) [n]: no

Use this configuration and save it? (yes/no) [y]: yes

[########################################] 100%


MDS Switch
h3csco9509 login:
```

Note: If you do confirm to save the configuration in the last step, none of your changes are updated until the next time the switch is rebooted. Ensure that you type **`yes`** here to save the new configuration.

The basic configuration is now finished, and we can proceed to upgrade the SAN-OS to the latest available level.

4.6.5 Upgrading SAN-OS

In this section we upgrade the SAN-OS to the latest released level. This can be done either using the CLI or the GUI (FM or DM). For completeness, we show how to perform the upgrade with both the CLI and the GUI.

Upgrading the SAN-OS using the CLI

Prior to upgrading the switch, we first list the current SAN-OS version running on the switch. Then we copy the SAN-OS code from a FTP server to the *bootflash:* on the switch as shown in Figure 4-4.

Example 4-4 Show the current SAN-OS version

```
h3csco9509# show version
Cisco Storage Area Networking Operating System (SAN-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2004, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  BIOS:      version 1.1.0
  loader:    version 1.0(3a)
  kickstart: version 2.0(3)
  system:    version 2.0(3)

  BIOS compile time:       10/24/03
  kickstart image file is: bootflash:///m9500-sf1ek9-kickstart-mz.2.0.3.bin
  kickstart compile time:  12/18/2004 21:00:00 [12/27/2004 19:07:38]
  system image file is:    bootflash:/m9500-sf1ek9-mz.2.0.3.bin
  system compile time:     12/18/2004 21:00:00 [12/27/2004 19:23:18]


Hardware
  RAM 1028776 kB
  bootflash: 500736 blocks (block size 512b)
  slot0:          0 blocks (block size 512b)

h3csco9509   uptime is 31 days 9 hours 9 minute(s) 59 second(s)

  Last reset
    Reason: Unknown
    System version: 2.0(3)
    Service:


h3csco9509# copy
ftp://9.42.166.193/teams/sc/m9500-sf1ek9-kickstart-mzg.3.0.0.270.bin.S1
bootflash:
Enter username: anonymous
Password:
h3csco9509# copy h3csco9509# copy
ftp://9.42.166.193/teams/sc/m9500-sf1ek9-mzg.3.0.0.270.bin.S1 bootflash:
Enter username: anonymous
Password:
h3csco9509#
```

We then verify that there is sufficient space on the remote supervisor bootflash, shown in Figure 4-5.

Example 4-5 Listing the bootflash: on the remote supervisor module

```
h3csco9509# dir bootflash://sup-remote
      12288     Jan 01 00:01:09 1980  lost+found/
   14397952     Jan 11 18:52:13 2005  m9500-sf1ek9-kickstart-mz.2.0.3.bin
   51436341     Jan 11 18:52:35 2005  m9500-sf1ek9-mz.2.0.3.bin

Usage for bootflash://sup-remote
   79849472 bytes used
  104710144 bytes free
  184559616 bytes total
h3csco9509#
```

Prior to starting the actual upgrade process, we back up the running configuration to our FTP server, as shown in Figure 4-6.

> **Note:** Best practice when performing configuration changes is always to save the running configuration to the startup configuration. As a way of operation, you could also preserve previous startup configurations for two generations.

Example 4-6 Backup the running configuration

```
h3csco9509# copy running-config
ftp://9.42.166.193/teams/sc/MDS3_h3csc09509_Nov08_2005
Enter username: anonymous
Password:
sc9216a#
```

After backing up the configuration, we start the upgrade using the **`install all`** command, shown in Example 4-7.

Example 4-7 Upgrading the director, using the **`install all`** *command*

```
h3csco9509# install all sys bootflash:/m9500-sf1ek9-mzg.3.0.0.270.bin.S1
kickstart bootflash:/m9500-sf1ek9-kickstart-mzg.3.0.0.270.bin.S1

Verifying image bootflash:/m9500-sf1ek9-kickstart-mzg.3.0.0.270.bin.S1
[####################] 100% -- SUCCESS

Verifying image bootflash:/m9500-sf1ek9-mzg.3.0.0.270.bin.S1
[####################] 100% -- SUCCESS

Extracting "slc" version from image
bootflash:/m9500-sf1ek9-mzg.3.0.0.270.bin.S1.
[####################] 100% -- SUCCESS

Extracting "system" version from image
bootflash:/m9500-sf1ek9-mzg.3.0.0.270.bin.S1.
[####################] 100% -- SUCCESS

Extracting "kickstart" version from image
bootflash:/m9500-sf1ek9-kickstart-mzg.3.0.0.270.bin.S1.
[####################] 100% -- SUCCESS

Extracting "loader" version from image
bootflash:/m9500-sf1ek9-kickstart-mzg.3.0.0.270.bin.S1.
[####################] 100% -- SUCCESS



Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes  non-disruptive       rolling
     2       yes  non-disruptive       rolling
     5       yes  non-disruptive         reset
     6       yes  non-disruptive         reset
```

```
Images will be upgraded according to following table:
Module       Image       Running-Version           New-Version  Upg-Required
------  ----------  --------------------  --------------------  ------------
     1         slc                2.0(3)                3.0(1)           yes
     1        bios      v1.1.0(10/24/03)      v1.1.0(10/24/03)            no
     2         slc                2.0(3)                3.0(1)           yes
     2        bios      v1.1.0(10/24/03)      v1.1.0(10/24/03)            no
     5      system                2.0(3)                3.0(1)           yes
     5   kickstart                2.0(3)                3.0(1)           yes
     5        bios      v1.1.0(10/24/03)      v1.1.0(10/24/03)            no
     5      loader               1.0(3a)                1.2(2)           yes
     6      system                2.0(3)                3.0(1)           yes
     6   kickstart                2.0(3)                3.0(1)           yes
     6        bios      v1.1.0(10/24/03)      v1.1.0(10/24/03)            no
     6      loader               1.0(3a)                1.2(2)           yes

Do you want to continue with the installation (y/n)?  [n]
Install is in progress, please wait.

Syncing image bootflash:/m9500-sf1ek9-kickstart-mzg.3.0.0.270.bin.S1 to
standby.
[####################] 100% -- SUCCESS

Syncing image bootflash:/m9500-sf1ek9-mzg.3.0.0.270.bin.S1 to standby.
[####################] 100% -- SUCCESS

Setting boot variables.
[####################] 100% -- SUCCESS

Performing configuration copy.
[####################] 100% -- SUCCESS

Module 5: Upgrading Bios/loader/bootrom.
[####################] 100% -- SUCCESS

Module 6: Upgrading Bios/loader/bootrom.
[####################] 100% -- SUCCESS

Module 6: Waiting for module online.
-- SUCCESS


"Switching over onto standby".
```

```
Reissuing Telnet

h3csco9509# show install all status
There is an on-going installation...
Enter Ctrl-C to go back to the prompt.

Continuing with installation, please wait

Module 6: Waiting for module online.
 -- SUCCESS
2005 Nov  9 05:01:47 h3csco9509 %IMAGE_DNLD-SLOT1-2-IMG_DNLD_STARTED:  Module
image download process. Please wait until completion...

Module 1: Non-disruptive upgrading.
2005 Nov  9 05:02:04 h3csco9509 %IMAGE_DNLD-SLOT1-2-IMG_DNLD_COMPLETE:  Module
image download process. Download successful.
2005 Nov  9 05:03:14 h3csco9509 %IMAGE_DNLD-SLOT2-2-IMG_DNLD_STARTED:  Module
image download process. Please wait until completion...
 -- SUCCESS

Module 2: Non-disruptive upgrading.
2005 Nov  9 05:03:29 h3csco9509 %IMAGE_DNLD-SLOT2-2-IMG_DNLD_COMPLETE:  Module
image download process. Download successful.
 -- SUCCESS

Install has been successful.
```

After the upgrade has completed, we verify the version using the command **`show version`** as shown in Example 4-8.

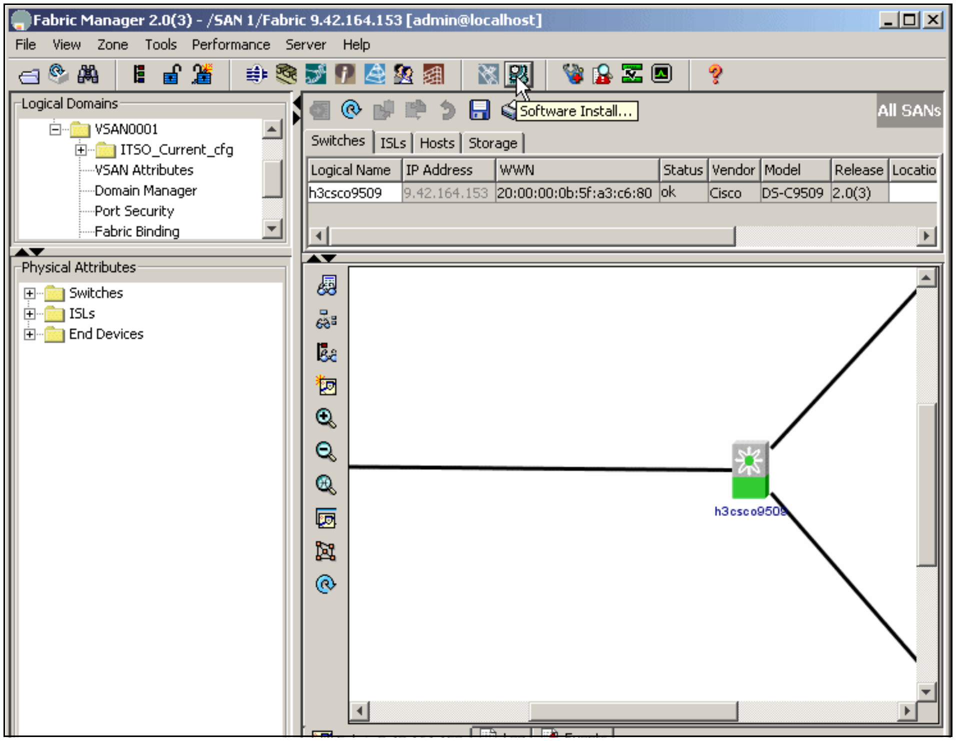
Example 4-8 Issuing **`show version`** *after upgrade*

```
h3csco9509# show version
Cisco Storage Area Networking Operating System (SAN-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2005, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  BIOS:      version 1.1.0
  loader:    version 1.2(2)
  kickstart: version 3.0(1) [build 3.0(0.270)] [gdb]
  system:    version 3.0(1) [build 3.0(0.270)] [gdb]

  BIOS compile time:       10/24/03
  kickstart image file is:
bootflash:///m9500-sf1ek9-kickstart-mzg.3.0.0.270.bin
.S1
  kickstart compile time:  10/12/2020 25:00:00 [11/01/2005 04:15:17]
  system image file is:    bootflash:/m9500-sf1ek9-mzg.3.0.0.270.bin.S1
  system compile time:     12/25/2010 12:00:00 [11/01/2005 05:13:38]


Hardware
  cisco MDS 9509 ("Supervisor/Fabric-1")
  Intel(R) Pentium(R) III CPU with 1028612 kB of memory.
  Processor Board ID JAB070204FG

  bootflash:  250368 kB
  slot0:           0 kB

h3csco9509   kernel uptime is 0 days 0 hour 10 minute(s) 26 second(s)

  Last reset
    Reason: Unknown
    System version: 2.0(3)
    Service:
```

Upgrading the SAN-OS using the GUI

In the following example, we upgrade a director using the GUI, invoking the process using the Fabric Manager interface.

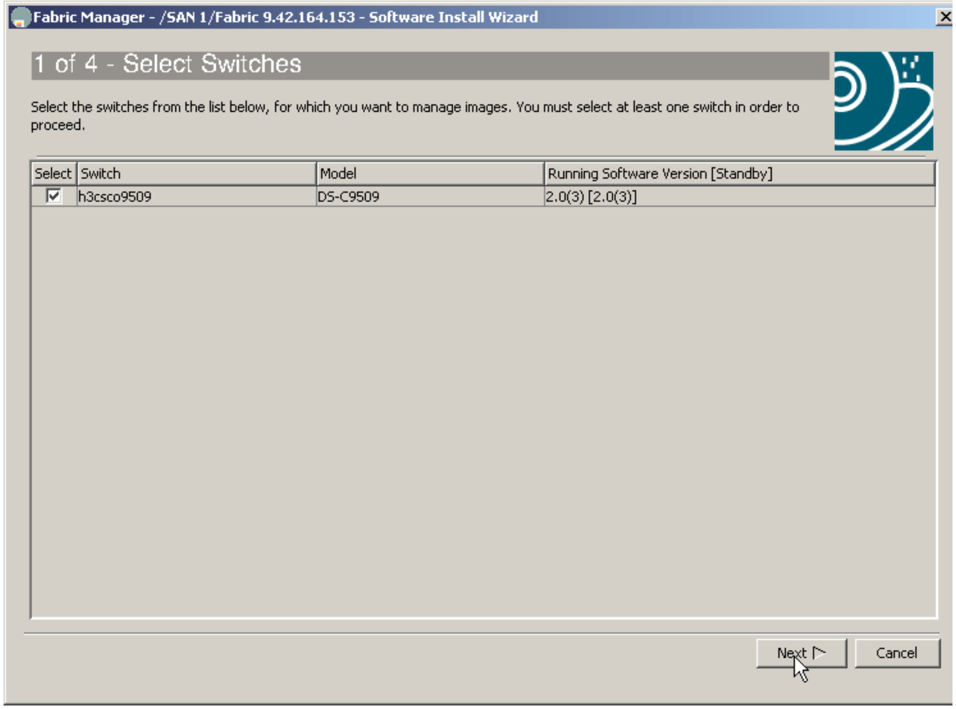
To start the process, we invoke the Fabric Manager Software install wizard by clicking the icon shown in Figure 4-20.


Fabric Manager 2.0(3) - /SAN 1/Fabric 9.42.164.153 [admin@localhost]
File
View
Zone
Tools
Performance
Server
Help
Logical Domains
VSAN0001
ITSO_Current_cfg
VSAN Attributes
Domain Manager
Port Security
Fabric Binding
Physical Attributes
Switches
ISLs
End Devices
Software Install...
All SANs
Switches
ISLs
Hosts
Storage
h3csco9509

Logical Name	IP Address	WWN	Status	Vendor	Model	Release	Locatio
h3csco9509	9.42.164.153	20:00:00:0b:5f:a3:c6:80	ok	Cisco	DS-C9509	2.0(3)	

Figure 4-20 Upgrade using Fabric Manager

In step 1, the Software Install wizard prompts us to select which switches we want to upgrade, and we click **Next** as shown in Figure 4-21.


Fabric Manager - /SAN 1/Fabric 9.42.164.153 - Software Install Wizard
1 of 4 - Select Switches

Select the switches from the list below, for which you want to manage images. You must select at least one switch in order to proceed.

Select	Switch	Model	Running Software Version [Standby]
☑	h3csco9509	DS-C9509	2.0(3) [2.0(3)]

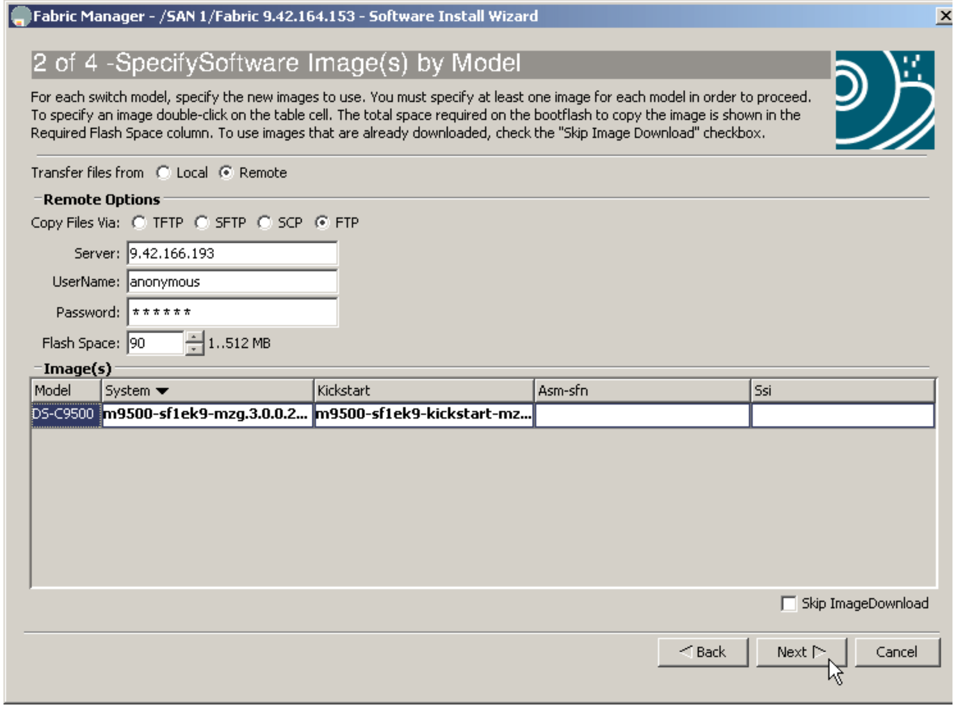
Next
Cancel

Figure 4-21 Selecting the switches to upgrade

In step 2, the wizard prompts for the location of the software we want to install. We specify the FTP server where the *kickstart* and *system* images reside, the size of the images and login credentials for the FTP server, and click **Next** shown in Figure 4-22.

Note: The complete path to the file location must be specified for this step to complete successfully.

The wizard does not verify if the images match the specified size, but the value is used to verify if the amount of corresponding free space is available on the bootflash, prior to initiating the download.



Fabric Manager - /SAN 1/Fabric 9.42.164.153 - Software Install Wizard

2 of 4 -SpecifySoftware Image(s) by Model

For each switch model, specify the new images to use. You must specify at least one image for each model in order to proceed. To specify an image double-click on the table cell. The total space required on the bootflash to copy the image is shown in the Required Flash Space column. To use images that are already downloaded, check the "Skip Image Download" checkbox.

Transfer files from ○ Local ● Remote

Remote Options

Copy Files Via: ○ TFTP ○ SFTP ○ SCP ● FTP

Server: 9.42.166.193

UserName: anonymous

Password: ******

Flash Space: 90 1..512 MB

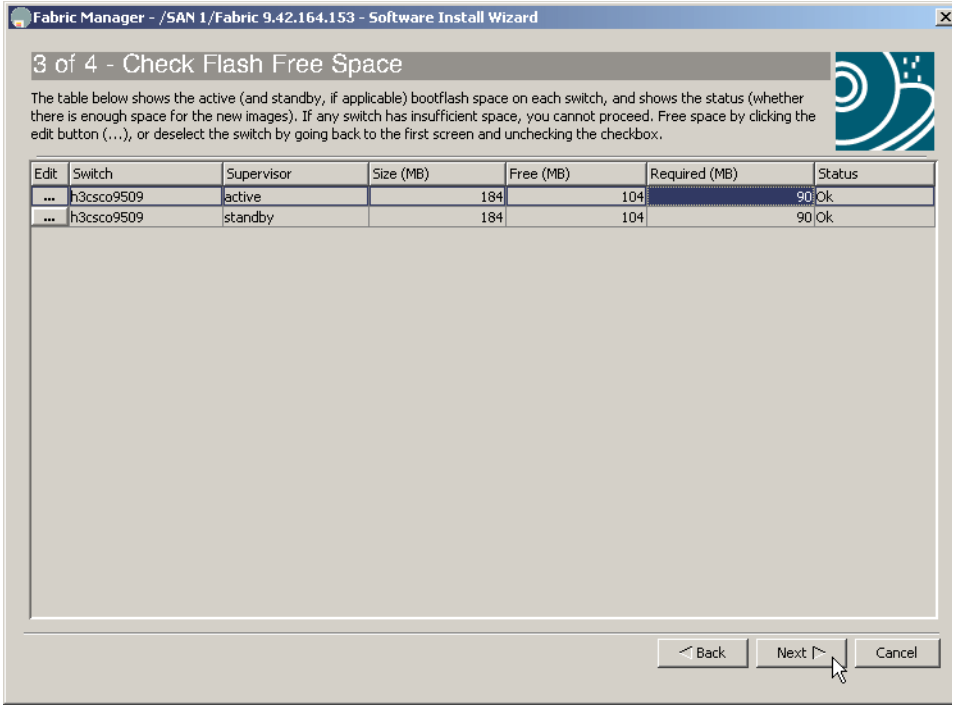
Image(s)

Model	System	Kickstart	Asm-sfn	Ssi
DS-C9500	m9500-sf1ek9-mzg.3.0.0.2...	m9500-sf1ek9-kickstart-mz...		

☐ Skip ImageDownload

Figure 4-22 Specifying images and location

In step 3, the software install wizard verifies if the required free space is available on the bootflash, and we click **Next**, as shown in Figure 4-23.


Fabric Manager - /SAN 1/Fabric 9.42.164.153 - Software Install Wizard

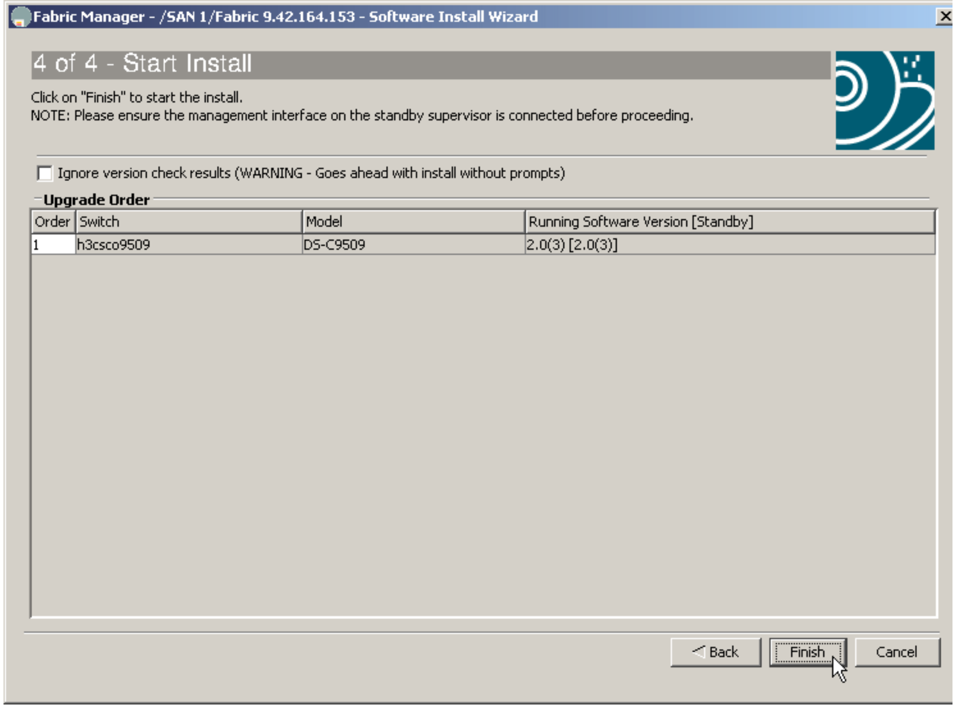
3 of 4 - Check Flash Free Space

The table below shows the active (and standby, if applicable) bootflash space on each switch, and shows the status (whether there is enough space for the new images). If any switch has insufficient space, you cannot proceed. Free space by clicking the edit button (...), or deselect the switch by going back to the first screen and unchecking the checkbox.

Edit	Switch	Supervisor	Size (MB)	Free (MB)	Required (MB)	Status
...	h3csco9509	active	184	104	90	Ok
...	h3csco9509	standby	184	104	90	Ok

Figure 4-23 Verifying required free space on bootflash

In step 4, we then start the installation as shown in Figure 4-24.


Fabric Manager - /SAN 1/Fabric 9.42.164.153 - Software Install Wizard

4 of 4 - Start Install

Click on "Finish" to start the install.
NOTE: Please ensure the management interface on the standby supervisor is connected before proceeding.

☐ Ignore version check results (WARNING - Goes ahead with install without prompts)

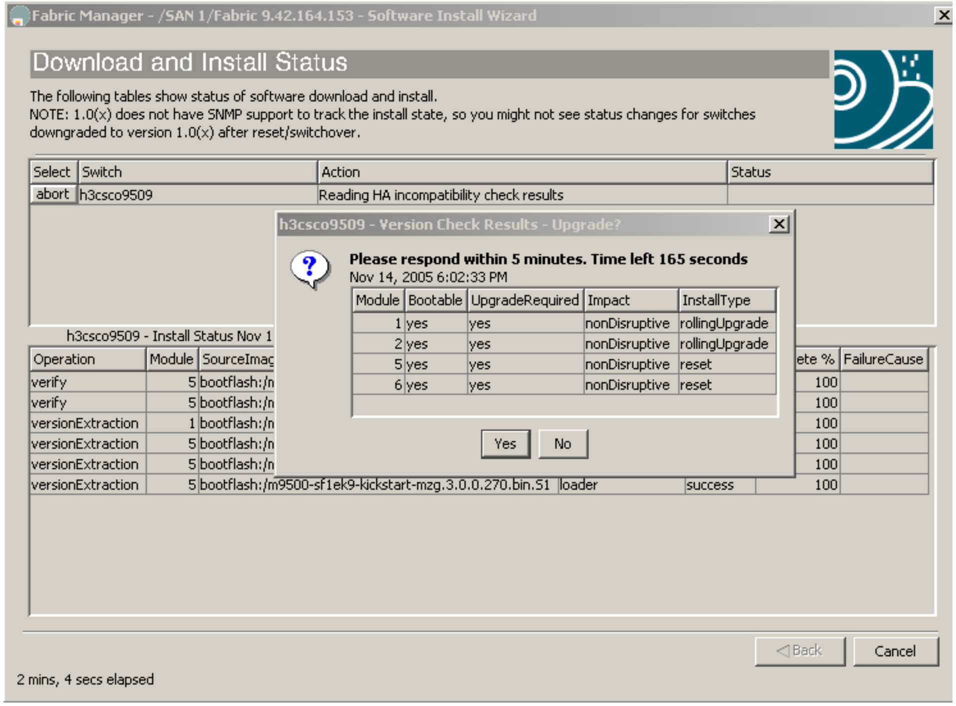
Upgrade Order

Order	Switch	Model	Running Software Version [Standby]
1	h3csco9509	DS-C9509	2.0(3) [2.0(3)]

< Back
Finish
Cancel

Figure 4-24 Starting the installation

In step 5, the image download starts, and upon completion, bootflash synchronization and compatibility checks are performed. When the wizard is ready to start the upgrade, we are prompted to click **Yes** (within a time-out period of 5 minutes) to start the upgrade, as shown in Figure 4-25.


Fabric Manager - /SAN 1/Fabric 9.42.164.153 - Software Install Wizard

Download and Install Status

The following tables show status of software download and install.
NOTE: 1.0(x) does not have SNMP support to track the install state, so you might not see status changes for switches downgraded to version 1.0(x) after reset/switchover.

Select	Switch	Action	Status
abort	h3csco9509	Reading HA incompatibility check results	

h3csco9509 - Version Check Results - Upgrade?

Please respond within 5 minutes. Time left 165 seconds
Nov 14, 2005 6:02:33 PM

Module	Bootable	UpgradeRequired	Impact	InstallType
1	yes	yes	nonDisruptive	rollingUpgrade
2	yes	yes	nonDisruptive	rollingUpgrade
5	yes	yes	nonDisruptive	reset
6	yes	yes	nonDisruptive	reset

h3csco9509 - Install Status Nov 1

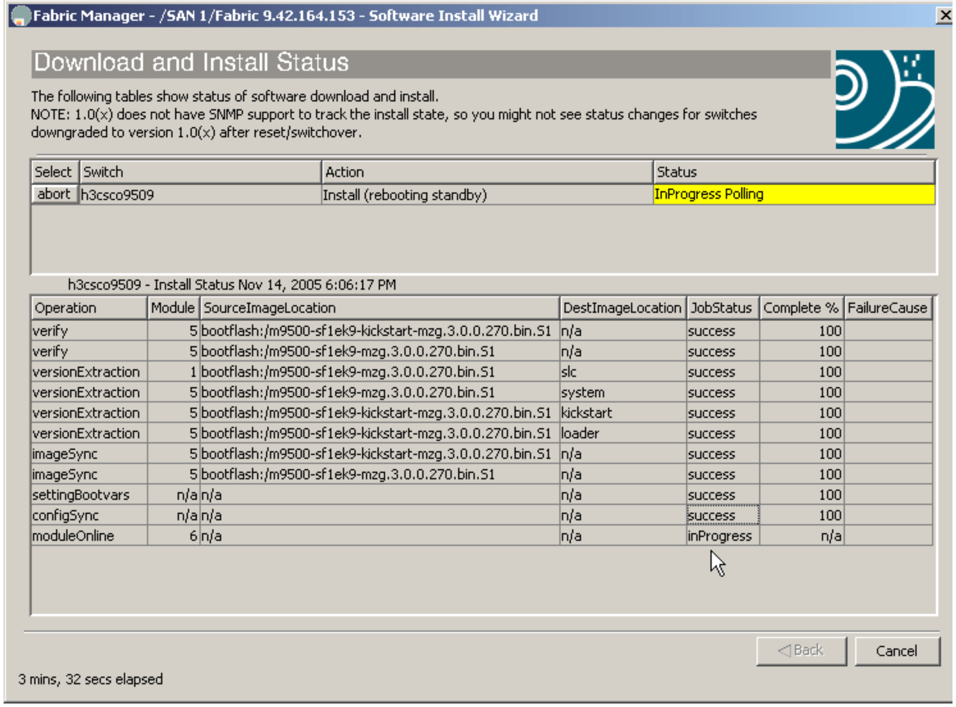
Operation	Module	SourceImag			ete %	FailureCause
verify	5	bootflash:/n			100	
verify	5	bootflash:/n			100	
versionExtraction	1	bootflash:/n			100	
versionExtraction	5	bootflash:/n			100	
versionExtraction	5	bootflash:/n			100	
versionExtraction	5	bootflash:/m9500-sf1ek9-kickstart-mzg.3.0.0.270.bin.S1	loader	success	100	

2 mins, 4 secs elapsed

Figure 4-25 Download and install status

Note: If you want to perform the upgrade unattended, in order to avoid being prompted to start the upgrade, you can check mark the **`Ignore versions check results`**, as shown in Figure 4-24.

In step 6, as the installation progresses, step-by-step status is continuously displayed as shown in Figure 4-26.


Fabric Manager - /SAN 1/Fabric 9.42.164.153 - Software Install Wizard

Download and Install Status

The following tables show status of software download and install.
NOTE: 1.0(x) does not have SNMP support to track the install state, so you might not see status changes for switches downgraded to version 1.0(x) after reset/switchover.

Select	Switch	Action	Status
abort	h3csco9509	Install (rebooting standby)	InProgress Polling

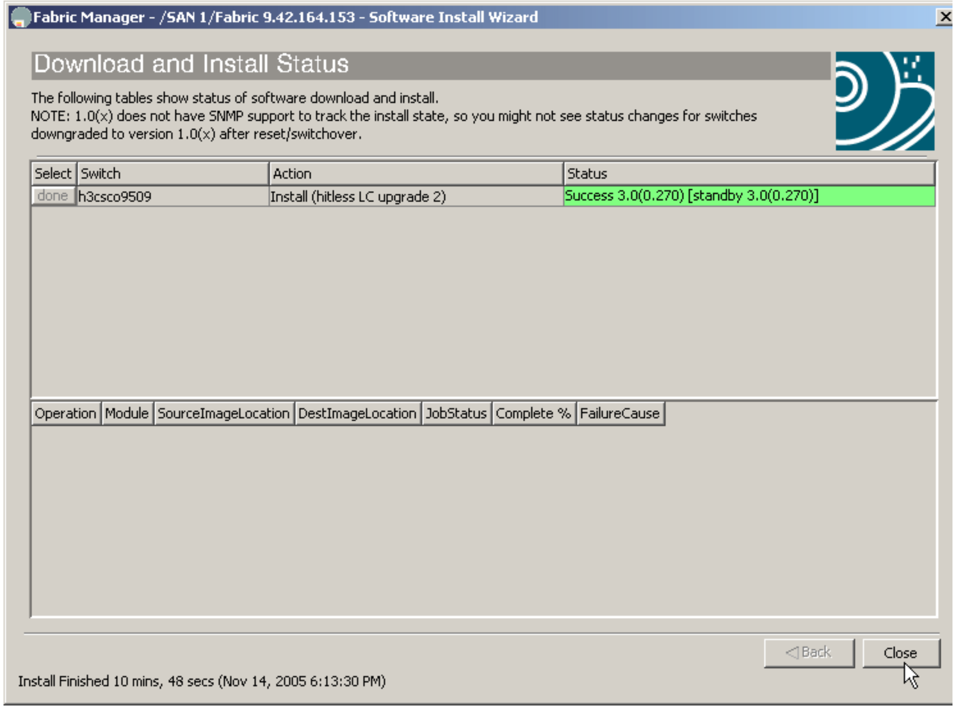
h3csco9509 - Install Status Nov 14, 2005 6:06:17 PM

Operation	Module	SourceImageLocation	DestImageLocation	JobStatus	Complete %	FailureCause
verify	5	bootflash:/m9500-sf1ek9-kickstart-mzg.3.0.0.270.bin.S1	n/a	success	100	
verify	5	bootflash:/m9500-sf1ek9-mzg.3.0.0.270.bin.S1	n/a	success	100	
versionExtraction	1	bootflash:/m9500-sf1ek9-mzg.3.0.0.270.bin.S1	slc	success	100	
versionExtraction	5	bootflash:/m9500-sf1ek9-mzg.3.0.0.270.bin.S1	system	success	100	
versionExtraction	5	bootflash:/m9500-sf1ek9-kickstart-mzg.3.0.0.270.bin.S1	kickstart	success	100	
versionExtraction	5	bootflash:/m9500-sf1ek9-kickstart-mzg.3.0.0.270.bin.S1	loader	success	100	
imageSync	5	bootflash:/m9500-sf1ek9-kickstart-mzg.3.0.0.270.bin.S1	n/a	success	100	
imageSync	5	bootflash:/m9500-sf1ek9-mzg.3.0.0.270.bin.S1	n/a	success	100	
settingBootvars	n/a	n/a	n/a	success	100	
configSync	n/a	n/a	n/a	success	100	
moduleOnline	6	n/a	n/a	inProgress	n/a	

3 mins, 32 secs elapsed

Figure 4-26 Monitoring installation progress

In step 7, when the installation completes, the status of the upgrade is displayed as shown in Figure 4-27.


Fabric Manager - /SAN 1/Fabric 9.42.164.153 - Software Install Wizard
Back
Close

Download and Install Status

The following tables show status of software download and install.
NOTE: 1.0(x) does not have SNMP support to track the install state, so you might not see status changes for switches downgraded to version 1.0(x) after reset/switchover.

Select	Switch	Action	Status
done	h3csco9509	Install (hitless LC upgrade 2)	Success 3.0(0.270) [standby 3.0(0.270)]

Operation	Module	SourceImageLocation	DestImageLocation	JobStatus	Complete %	FailureCause

Install Finished 10 mins, 48 secs (Nov 14, 2005 6:13:30 PM)

Figure 4-27 Upgrade completed

4.6.6 Managing licenses

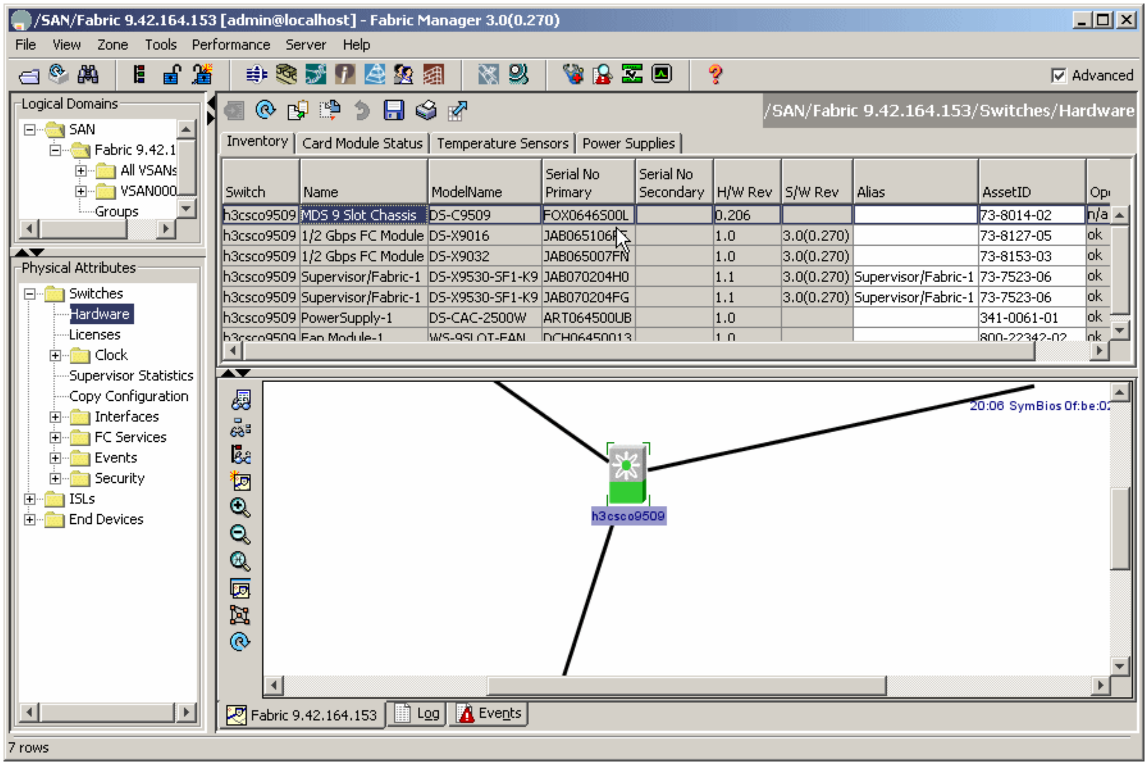
To obtain new or updated license key files, follow these steps:

1. Collect the host ID of the switch, also referred to as the switch serial number, using the command **`show license host-id`** from the CLI as shown in Example 4-9; the host id is *FOX0646S00*.

Example 4-9 Listing the switch serial number

```
h3csco9509# show license host-id
License hostid: VDH=FOX0646S00L
```

This can also be done using the GUI as shown in Figure 4-28; the switch **Serial No Primary** is equivalent to the License hostid.


/SAN/Fabric 9.42.164.153 [admin@localhost] - Fabric Manager 3.0(0.270)
File View Zone Tools Performance Server Help
Advanced
Logical Domains
SAN
Fabric 9.42.1
All VSANs
VSAN000
Groups
Physical Attributes
Switches
Hardware
Licenses
Clock
Supervisor Statistics
Copy Configuration
Interfaces
FC Services
Events
Security
ISLs
End Devices
/SAN/Fabric 9.42.164.153/Switches/Hardware
Inventory
Card Module Status
Temperature Sensors
Power Supplies
20:06 SymBios 0f:be:0
h3csco9509
Fabric 9.42.164.153
Log
Events
7 rows

Switch	Name	ModelName	Serial No Primary	Serial No Secondary	H/W Rev	S/W Rev	Alias	AssetID	Op
h3csco9509	MDS 9 Slot Chassis	DS-C9509	FOX0646500L		0.206			73-8014-02	n/a
h3csco9509	1/2 Gbps FC Module	DS-X9016	JAB065106		1.0	3.0(0.270)		73-8127-05	ok
h3csco9509	1/2 Gbps FC Module	DS-X9032	JAB065007FN		1.0	3.0(0.270)		73-8153-03	ok
h3csco9509	Supervisor/Fabric-1	DS-X9530-SF1-K9	JAB070204H0		1.1	3.0(0.270)	Supervisor/Fabric-1	73-7523-06	ok
h3csco9509	Supervisor/Fabric-1	DS-X9530-SF1-K9	JAB070204FG		1.1	3.0(0.270)	Supervisor/Fabric-1	73-7523-06	ok
h3csco9509	PowerSupply-1	DS-CAC-2500W	ART064500UB		1.0			341-0061-01	ok
h3csco9509	Fan Module-1	WS-9SLOT-FAN	DCH06450013		1.0			800-22342-02	ok

Figure 4-28 Listing the serial number

2. Obtain your Claim Certificate or the Proof of Purchase document.
3. Locate the Product Authorization Key (PAK) from the Claim Certificate or Proof of Purchase document.
4. Locate the Web site URL from the Claim Certificate or Proof of Purchase document.
5. Access the specified URL that applies to your switch and enter the switch serial number and the PAK.

The license key file is sent to you by e-mail. The license key file is digitally signed to only authorize use on the switch for which it was requested. The requested features are also enabled once the SAN-OS software on the specified switch accesses the license key file.

When you have received your digitally signed license key(s), they can now be installed on the switch. The license files can be copied to the switch bootflash beforehand, or they can be copied during the install process.

View installed licenses

To list installed licenses on a switch, you can issue the command **`show license`** from the CLI or from the Device Manager select **Admin** → **Licenses** shown in Figure 4-29.

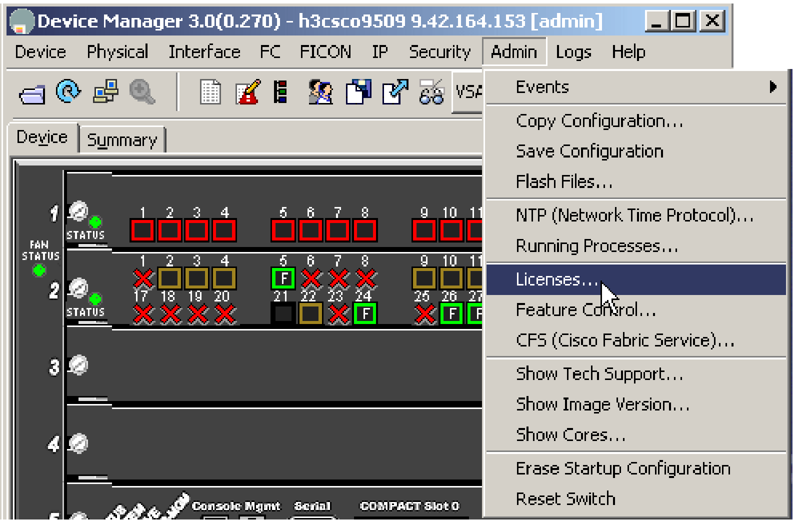
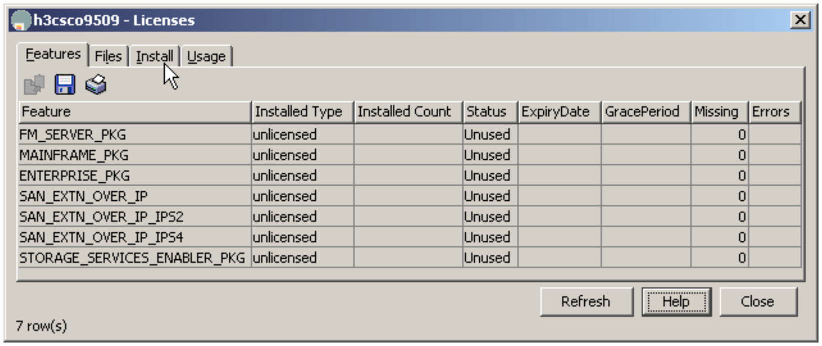

Device Manager 3.0(0.270) - h3csco9509 9.42.164.153 [admin]
Device
Physical
Interface
FC
FICON
IP
Security
Admin
Logs
Help
Device
Summary
Events
Copy Configuration...
Save Configuration
Flash Files...
NTP (Network Time Protocol)...
Running Processes...
Licenses...
Feature Control...
CFS (Cisco Fabric Service)...
Show Tech Support...
Show Image Version...
Show Cores...
Erase Startup Configuration
Reset Switch
FAN STATUS
STATUS
Console Mgmt
Serial
COMPACT Slot 0

Figure 4-29 Selecting the licensing interface

The list of available license features are listed, as well as the properties for each feature. We see that we currently have not installed any licenses on the switch, as shown in Figure 4-30.


h3csco9509 - Licenses
Features
Files
Install
Usage
Refresh
Help
Close

Feature	Installed Type	Installed Count	Status	ExpiryDate	GracePeriod	Missing	Errors
FM_SERVER_PKG	unlicensed		Unused			0	
MAINFRAME_PKG	unlicensed		Unused			0	
ENTERPRISE_PKG	unlicensed		Unused			0	
SAN_EXTN_OVER_IP	unlicensed		Unused			0	
SAN_EXTN_OVER_IP_IPS2	unlicensed		Unused			0	
SAN_EXTN_OVER_IP_IPS4	unlicensed		Unused			0	
STORAGE_SERVICES_ENABLER_PKG	unlicensed		Unused			0	

7 row(s)

Figure 4-30 Displaying installed licenses

Copying files to the bootflash using the Device Manager

Prior to applying a license file, we upload it to the bootflash. In Figure 4-31 we select **Admin** → **Flash Files** in the device manager to invoke the *Flash Files* interface.

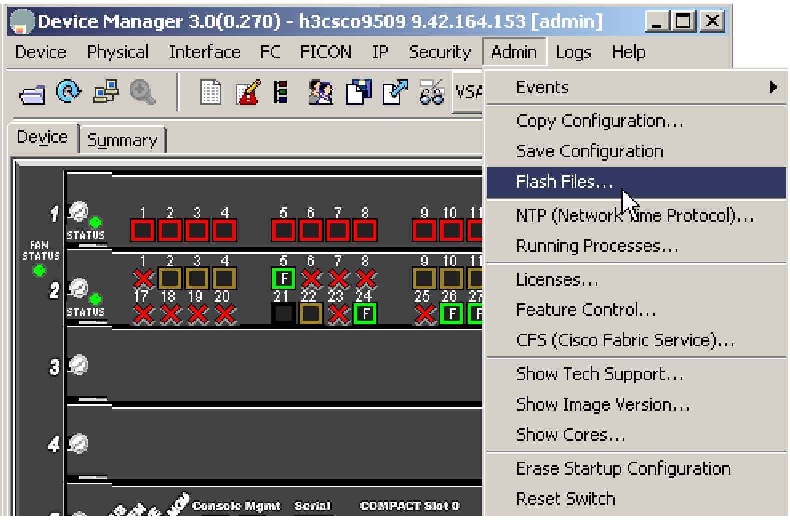
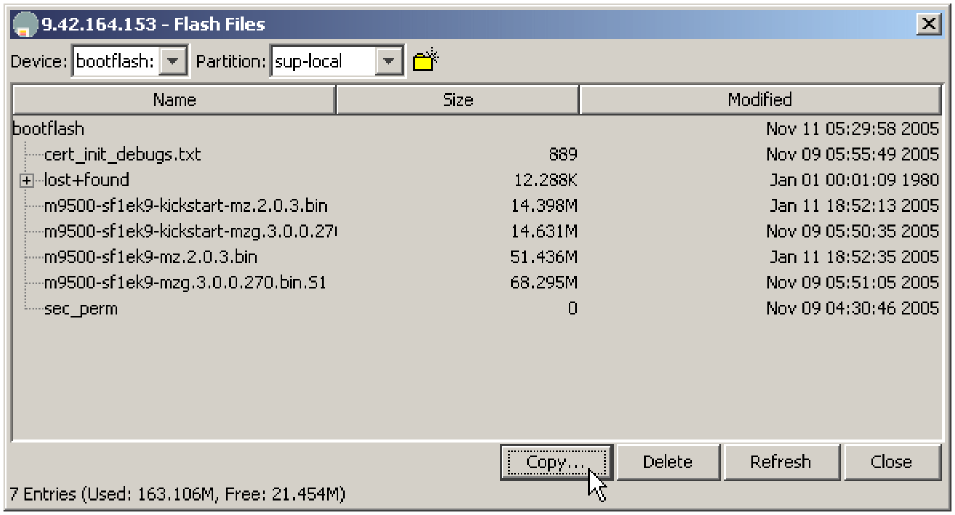

Device Manager 3.0(0.270) - h3csco9509 9.42.164.153 [admin]
Device
Physical
Interface
FC
FICON
IP
Security
Admin
Logs
Help
Device
Summary
Events
Copy Configuration...
Save Configuration
Flash Files...
NTP (Network Time Protocol)...
Running Processes...
Licenses...
Feature Control...
CFS (Cisco Fabric Service)...
Show Tech Support...
Show Image Version...
Show Cores...
Erase Startup Configuration
Reset Switch
FAN STATUS
STATUS
Console Mgmt
Serial
COMPACT Slot 0

Figure 4-31 Starting the Flash Files interface

The Flash Files interface is initialized as shown in Figure 4-32, and we select the **Copy** option.


9.42.164.153 - Flash Files
Copy...
Delete
Refresh
Close

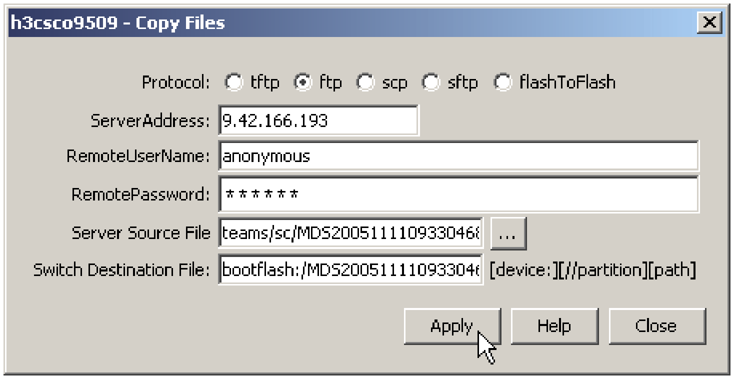
Device: bootflash: Partition: sup-local

Name	Size	Modified
bootflash		Nov 11 05:29:58 2005
cert_init_debugs.txt	889	Nov 09 05:55:49 2005
lost+found	12.288K	Jan 01 00:01:09 1980
m9500-sf1ek9-kickstart-mz.2.0.3.bin	14.398M	Jan 11 18:52:13 2005
m9500-sf1ek9-kickstart-mzg.3.0.0.27	14.631M	Nov 09 05:50:35 2005
m9500-sf1ek9-mz.2.0.3.bin	51.436M	Jan 11 18:52:35 2005
m9500-sf1ek9-mzg.3.0.0.270.bin.S1	68.295M	Nov 09 05:51:05 2005
sec_perm	0	Nov 09 04:30:46 2005

7 Entries (Used: 163.106M, Free: 21.454M)

Figure 4-32 Selecting the copy option

When selecting the Copy option, we are prompted to define the transfer protocol, server address, login credentials, and the source and target file names, and once done, we click **Apply** to start the copy.



Protocol: ○ tftp ● ftp ○ scp ○ sftp ○ flashToFlash

ServerAddress: 9.42.166.193

RemoteUserName: anonymous

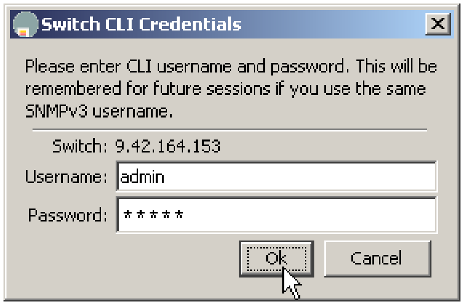
RemotePassword: ******

Server Source File: teams/sc/MDS200511110933046

Switch Destination File: bootflash:/MDS20051111093304 [device:][//partition][path]

Figure 4-33 Specifying file to copy

> **Note:** During the execution of tasks using Device Manager, we are occasionally prompted to provide CLI login credentials. This is because the Java applet issues the commands towards the SAN-OS using the CLI, as shown in Figure 4-34.



Please enter CLI username and password. This will be remembered for future sessions if you use the same SNMPv3 username.

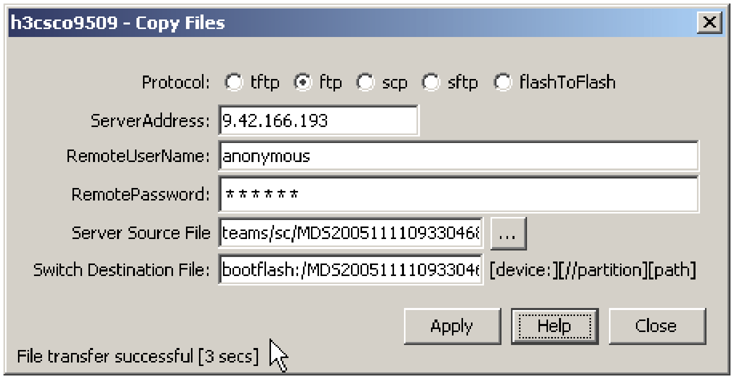
Switch: 9.42.164.153

Username: admin

Password: *****

Figure 4-34 Entering login credentials for the CLI

Copy status notification is displayed in the bottom left of the *Copy Files* window, and upon completion we are notified that the file transfer was successful, as shown in Figure 4-35.



Protocol: ○ tftp ● ftp ○ scp ○ sftp ○ flashToFlash
ServerAddress: 9.42.166.193
RemoteUserName: anonymous
RemotePassword: ******
Server Source File teams/sc/MDS200511110933046
Switch Destination File: bootflash:/MDS20051111093304 [device:][//partition][path]

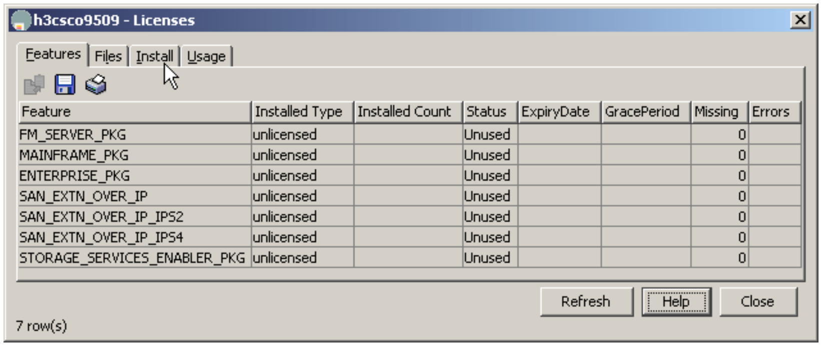
File transfer successful [3 secs]

Figure 4-35 File transfer completed successfully.

We have now transferred the license file to the bootflash, and we can proceed with installation of the license feature.

Installing a license using the Device Manager

To install a license on the switch, we select the **Install** tab.

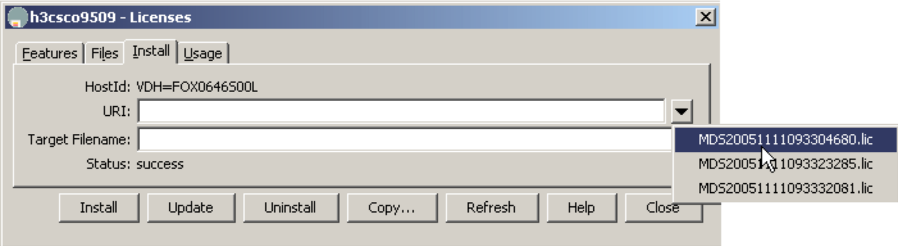


Feature	Installed Type	Installed Count	Status	ExpiryDate	GracePeriod	Missing	Errors
FM_SERVER_PKG	unlicensed		Unused			0	
MAINFRAME_PKG	unlicensed		Unused			0	
ENTERPRISE_PKG	unlicensed		Unused			0	
SAN_EXTN_OVER_IP	unlicensed		Unused			0	
SAN_EXTN_OVER_IP_IPS2	unlicensed		Unused			0	
SAN_EXTN_OVER_IP_IPS4	unlicensed		Unused			0	
STORAGE_SERVICES_ENABLER_PKG	unlicensed		Unused			0	

7 row(s)

Figure 4-36 Selecting the Install pane

On the **Install** tab, we click the pull-down icon to display available license files (in the bootflash), as shown in Figure 4-37.


h3csco9509 - Licenses
Features
Files
Install
Usage
Install
Update
Uninstall
Copy...
Refresh
Help
Close

HostId: VDH=FOX0646S00L

URI:

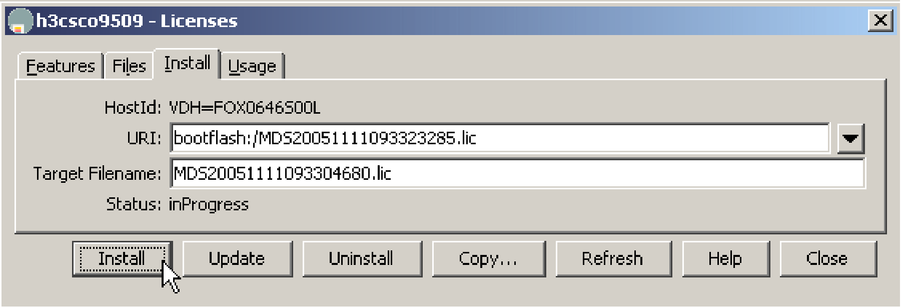
Target Filename:

Status: success

MDS20051111093304680.lic
MDS20051111093323285.lic
MDS20051111093332081.lic

Figure 4-37 Selecting the license file to install

We then click **Install** to start the license file installation as shown in Figure 4-38.


h3csco9509 - Licenses
Features
Files
Install
Usage
Install
Update
Uninstall
Copy...
Refresh
Help
Close

HostId: VDH=FOX0646S00L

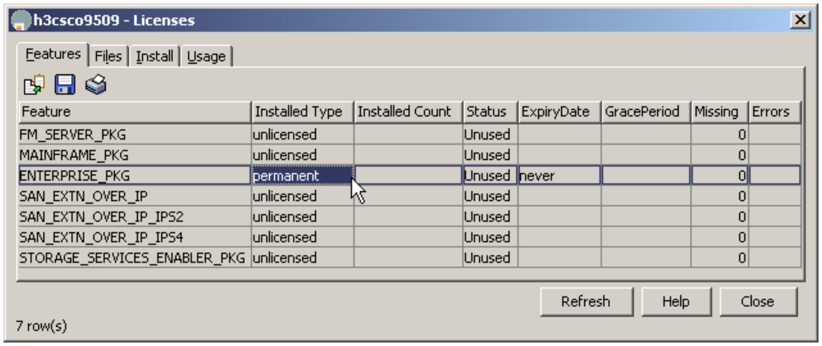
URI: bootflash:/MDS20051111093323285.lic

Target Filename: MDS20051111093304680.lic

Status: inProgress

Figure 4-38 Installing the license file

Upon completion of the license file installation, we click **Refresh** on the feature tab, and we verify that the desired feature has been activated, as shown in Figure 4-39.


h3csco9509 - Licenses
Features
Files
Install
Usage
Refresh
Help
Close
7 row(s)

Feature	Installed Type	Installed Count	Status	ExpiryDate	GracePeriod	Missing	Errors
FM_SERVER_PKG	unlicensed		Unused			0	
MAINFRAME_PKG	unlicensed		Unused			0	
ENTERPRISE_PKG	permanent		Unused	never		0	
SAN_EXTN_OVER_IP	unlicensed		Unused			0	
SAN_EXTN_OVER_IP_IPS2	unlicensed		Unused			0	
SAN_EXTN_OVER_IP_IPS4	unlicensed		Unused			0	
STORAGE_SERVICES_ENABLER_PKG	unlicensed		Unused			0	

Figure 4-39 Verifying the desired feature is activated

Installing a license using the CLI

First we copy the license to the bootflash: as shown in Example 4-10.

Example 4-10 Copy license file to the bootflash:

```
h3csco9509# copy ftp://9.42.166.193/teams/sc/MDS20051111093304680.lic
bootflash:
Enter username: anonymous
Password:
3csco9509#
```

Subsequently we install the received license on the switch and then display the installed licenses, as shown in Example 4-11.

Example 4-11 Installing the Fabric Manager Server license

```
h3csco9509# show license
h3csco9509# install license bootflash:/MDS20051111093304680.lic
Installing license ...............done
h3csco9509# sho license
MDS20051111093304680.lic:
SERVER this_host ANY
VENDOR cisco
INCREMENT FM_SERVER_PKG cisco 1.0 permanent uncounted \
        VENDOR_STRING=<LIC_SOURCE>MDS_SWIFT</LIC_SOURCE><SKU>M9500FMS1K9=</SKU>
\
        HOSTID=VDH=FOX0646S00L \

NOTICE="<LicFileID>20051111093304680</LicFileID><LicLineID>1</LicLineID>
 \
        <PAK></PAK>" SIGN=0B064A4AE3C8

h3csco9509#
```

4.6.7 Managing users

When accessing Cisco MDS 9000 family switches, you are required to authenticate with a username and a password, after which access is granted and role based authorization is applied.

Note: It is possible to disable login authentication, although this is *not* recommended.

Authentication

User authentication can be configured to be performed locally on the switch (in the lookup database) or remotely using one or more RADIUS or TACACS+ servers.

In the following topics, we authenticate using local authentication. For detailed information on how to set up remote authentication (RADIUS or TACACS+) consult the MDS config-guide:

`http://www.cisco.com/en/US/products/ps5989/products_installation_and_configuration_guides_list.html`

Authorization

By default the two roles *network-operator* and *network-admin* exist in all Cisco MDS 9000 family switches, and cannot be changed or deleted, although you can create other roles:

- **Network-operator**

  Has permission to view the configuration only and cannot make any configuration changes.

- **Network-admin**

  Has permission to execute all commands and configuration changes. The administrator has the permission to create (up to 64) additional roles.

Creating roles

To create a role, we define the name of the role and the profile, which specifies the permissions for the role. In Example 4-12 we create the role ITSO_admin and give this administrator access only to VSANs 50 to 60.

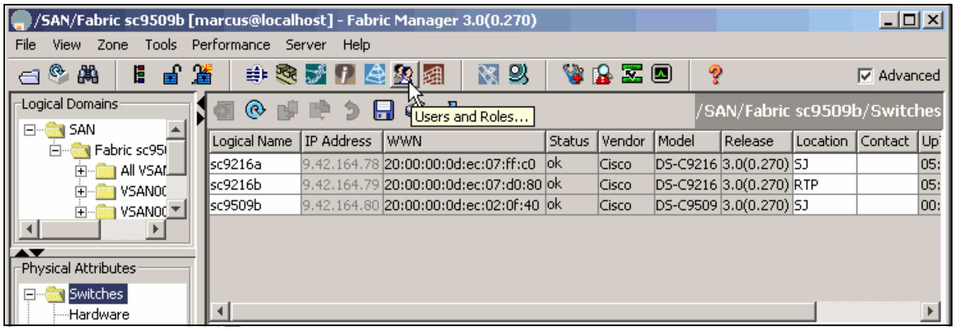
Finally, we issue the command **`show role`** to list defined roles.

Example 4-12 Creating a VSAN role

```
sc9509b# config t
Enter configuration commands, one per line.  End with CNTL/Z.
sc9509b(config)# role name ITSO_role
sc9509b(config-role)# description admin for VSAN50-VSAN60
sc9509b(config-role)# role name ITSO_role
sc9509b(config-role)# vsan policy deny
sc9509b(config-role-vsan)# permit vsan 50-60

sc9509b# show role
Role: network-admin
Description: Predefined Network Admin group. This role cannot be modified
Access to all the switch commands
```

```
Role: network-operator
Description: Predefined Network Operator group. This role cannot be modified
Access to Show commands and selected Exec commands


Role: svc-admin
Description: Predefined SVC Admin group. This role cannot be modified
Access to all SAN Volume Controller commands


Role: svc-operator
Description: Predefined SVC Operator group. This role cannot be modified
Access to selected SAN Volume Controller commands


Role: default-role
  Description: This is a system defined role and applies to all users
  vsan policy: permit (default)
  ---------------------------------------------
  Rule    Type    Command-type      Feature
  ---------------------------------------------
    1.   permit      show             system
    2.   permit      show               snmp
    3.   permit      show             module
    4.   permit      show           hardware
    5.   permit      show        environment


Role: ITSO_role
Description: admin for VSAN50-VSAN60
  vsan policy: deny
  Permitted vsans: 50-60
```

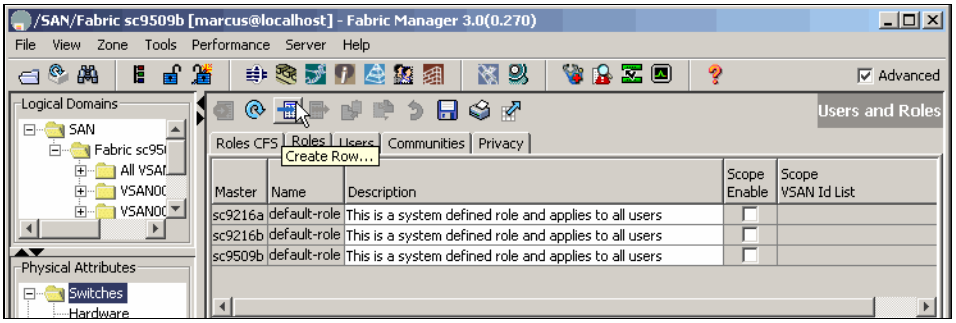
To perform the same configuration using Fabric Manager, we click the **Users and Roles** icon as shown in Figure 4-40.


/SAN/Fabric sc9509b [marcus@localhost] - Fabric Manager 3.0(0.270)
File View Zone Tools Performance Server Help
Advanced
Logical Domains
SAN
Fabric sc95
All VSAN
VSAN0C
VSAN0C
Physical Attributes
Switches
Hardware
Users and Roles...
/SAN/Fabric sc9509b/Switches

Logical Name	IP Address	WWN	Status	Vendor	Model	Release	Location	Contact	Up
sc9216a	9.42.164.78	20:00:00:0d:ec:07:ff:c0	ok	Cisco	DS-C9216	3.0(0.270)	SJ		05:
sc9216b	9.42.164.79	20:00:00:0d:ec:07:d0:80	ok	Cisco	DS-C9216	3.0(0.270)	RTP		05:
sc9509b	9.42.164.80	20:00:00:0d:ec:02:0f:40	ok	Cisco	DS-C9509	3.0(0.270)	SJ		00:

Figure 4-40 Selecting users and roles

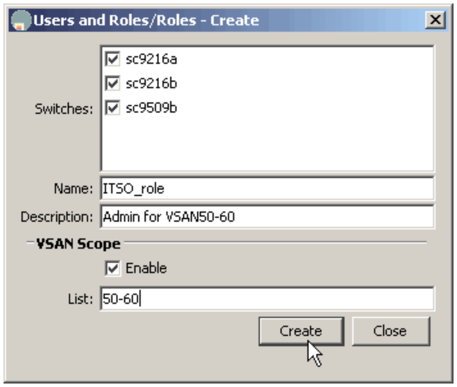
We then select the **Roles** tab and click the **Create Row** icon as shown in Figure 4-41.


/SAN/Fabric sc9509b [marcus@localhost] - Fabric Manager 3.0(0.270)
File View Zone Tools Performance Server Help
Advanced
Logical Domains
SAN
Fabric sc95
All VSAN
VSAN0C
VSAN0C
Physical Attributes
Switches
Hardware
Users and Roles
Roles CFS
Roles
Users
Communities
Privacy
Create Row...

Master	Name	Description	Scope Enable	Scope VSAN Id List
sc9216a	default-role	This is a system defined role and applies to all users	☐	
sc9216b	default-role	This is a system defined role and applies to all users	☐	
sc9509b	default-role	This is a system defined role and applies to all users	☐	

Figure 4-41 Selecting `Create Row`

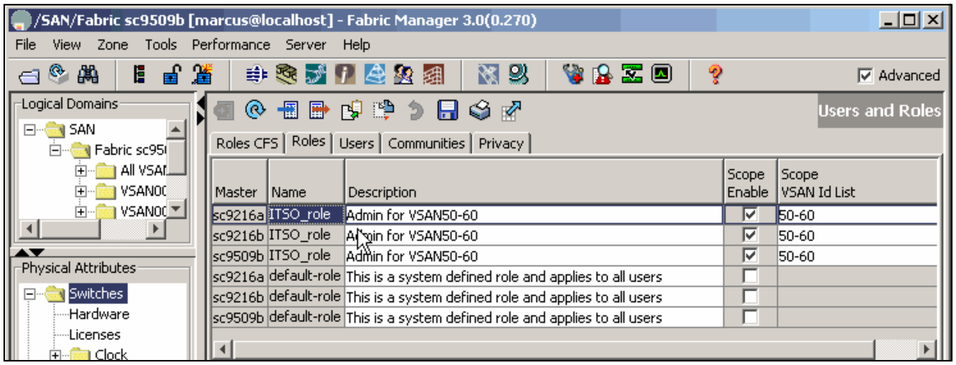
In the role creation window, we define the name of the role and the VSAN properties as shown in Figure 4-42, and click **Create**.


Users and Roles/Roles - Create
Create
Close

Switches: ☑ sc9216a
☑ sc9216b
☑ sc9509b
Name: ITSO_role
Description: Admin for VSAN50-60
VSAN Scope
☑ Enable
List: 50-60

Figure 4-42 Defining a new role

After closing the role creation window, we see that the created role is now listed, as shown in Figure 4-43.


/SAN/Fabric sc9509b [marcus@localhost] - Fabric Manager 3.0(0.270)
File
View
Zone
Tools
Performance
Server
Help
☑ Advanced
Logical Domains
SAN
Fabric sc95
All VSAN
VSAN0C
VSAN0C
Physical Attributes
Switches
Hardware
Licenses
Clock
Users and Roles
Roles CFS
Roles
Users
Communities
Privacy

Master	Name	Description	Scope Enable	Scope VSAN Id List
sc9216a	ITSO_role	Admin for VSAN50-60	☑	50-60
sc9216b	ITSO_role	Admin for VSAN50-60	☑	50-60
sc9509b	ITSO_role	Admin for VSAN50-60	☑	50-60
sc9216a	default-role	This is a system defined role and applies to all users	☐	
sc9216b	default-role	This is a system defined role and applies to all users	☐	
sc9509b	default-role	This is a system defined role and applies to all users	☐	

Figure 4-43 Listing the defined roles

Creating users

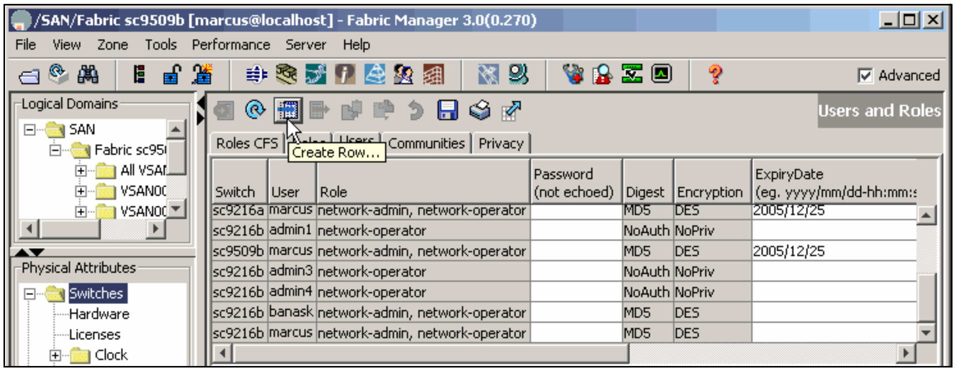
To create a user we define the name of the user and the profile(s), which specifies the permissions for the user. In Example 4-12 we create the role ITSO_user and apply the ITSO_role to this administrator, which only has permissions for VSANs 50 to 60.

Example 4-13 Creating a user

```
sc9509b# config t
Enter configuration commands, one per line.  End with CNTL/Z.
sc9509b(config)# username ITSO_user password a1b2c3d4 role ITSO_role

sc9509b# show user-account
user:admin
        this user account has no expiry date
        roles:network-admin

user:marcus
        expires on Sun Dec 25 23:59:59 2005
        roles:network-operator network-admin

user:ITSO_user
        this user account has no expiry date
        roles:ITSO_role
```

To create the same user using Fabric Manager, we click the **Users and Roles** icon as shown before in Figure 4-40 on page 783.

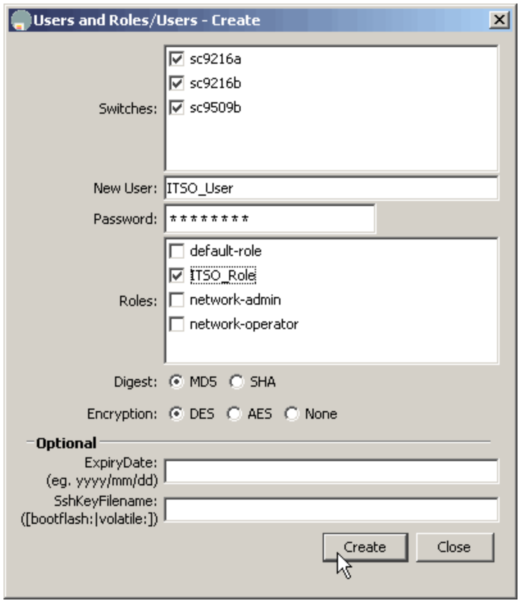
We then select the **Users** tab and click the **Create Row** icon as shown in Figure 4-44.


/SAN/Fabric sc9509b [marcus@localhost] - Fabric Manager 3.0(0.270)
File
View
Zone
Tools
Performance
Server
Help
Advanced
Logical Domains
SAN
Fabric sc95
All VSAI
VSAN0C
VSAN0C
Physical Attributes
Switches
Hardware
Licenses
Clock
Users and Roles
Roles CFS
Communities
Privacy
Create Row...

Switch	User	Role	Password (not echoed)	Digest	Encryption	ExpiryDate (eg. yyyy/mm/dd-hh:mm:s
sc9216a	marcus	network-admin, network-operator		MD5	DES	2005/12/25
sc9216b	admin1	network-operator		NoAuth	NoPriv	
sc9509b	marcus	network-admin, network-operator		MD5	DES	2005/12/25
sc9216b	admin3	network-operator		NoAuth	NoPriv	
sc9216b	admin4	network-operator		NoAuth	NoPriv	
sc9216b	banask	network-admin, network-operator		MD5	DES	
sc9216b	marcus	network-admin, network-operator		MD5	DES	

Figure 4-44 Selecting **`Create Row`**

In the user creation window we define the name of the user and the role(s) to apply as shown in Figure 4-45, and click **Create**.


Users and Roles/Users - Create
Optional
Create
Close

Switches: ☑ sc9216a ☑ sc9216b ☑ sc9509b

New User: ITSO_User

Password: ********

Roles: ☐ default-role ☑ ITSO_Role ☐ network-admin ☐ network-operator

Digest: ● MD5 ○ SHA

Encryption: ● DES ○ AES ○ None

ExpiryDate: (eg. yyyy/mm/dd)

SshKeyFilename: ([bootflash:|volatile:])

Figure 4-45 Creating a new user

As you can see, we have the option to define an expiry date for the user we create. To delete a user, we simply delete the row of the user to be deleted.

For further details on user and host creation, consult the MDS Cisco config guide:

http://www.cisco.com/en/US/products/ps5989/products_installation_and_configuration_guides_list.html

4.6.8 VSAN

A Virtual Storage Area Network (VSAN) is a unique feature of Cisco MDS 9000 family that enables dividing the physical Fibre Channel fabric to virtual SAN fabrics. Each VSAN is a completely separate SAN fabric, with its own set of domain IDs, fabric services, zones, namespace, and interoperability mode.

Each port in the switch fabric belongs to exactly one of the VSANs at any given time, with the exception of trunking E_Ports (TE_Ports) that can multiplex the traffic of several VSANs over a single physical link.

Up to 256 VSANs can be configured in a single switch. The VSAN numbers can range from 1 to 4094. VSAN number 1 is called the default VSAN, and is the VSAN that initially contains all of the ports in the switch. If you do not have to divide the fabric into VSANs, you can leave all ports in the default VSAN.

The VSAN number 4094 is called the isolated VSAN, and any port configured into that VSAN is isolated from all other ports. If you delete a VSAN, all ports in it are moved to the isolated VSAN to avoid implicit transfer of the ports to the default VSAN.

Note: Best practice for a large SAN environment is not to use VSAN1 while disallowing communication between ports that are not defined in a zone (at setup this is defined as default zone policy `deny`) and additionally not define any zones in VSAN1. Doing this prevents any accidental communication of new devices or hosts attached to the fabric since they by default belong to VSAN1.

Creating a VSAN using the CLI

When creating a VSAN, we assign a VSAN id and (optional) name which must be unique. In Example 4-14 we create VSAN 11 and name it *VSAN11*, using the default setting for interoperability and load balancing, then suspend it. After creating the VSAN, we list the defined VSANs.

Example 4-14 Creating a VSAN

```
sc9216b(config)# vsan database
sc9216b(config-vsan-db)# vsan 11
sc9216b(config-vsan-db)# vsan 11 name VSAN11
sc9216b(config-vsan-db)# vsan 11 suspend
sc9216b(config-vsan-db)# end

sc9216b# show vsan
vsan 1 information
         name:VSAN0001  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 11 information
         name:VSAN11  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 4094:isolated_vsan
```

Assigning ports to a VSAN

Now that we have created the VSAN we assign membership to the VSAN of the ports *fc1/1 and fc1/16* to VSAN 11 and afterwards we list the VSAN memberships, as shown in Example 4-15.

Example 4-15 Assigning membership to a VSAN

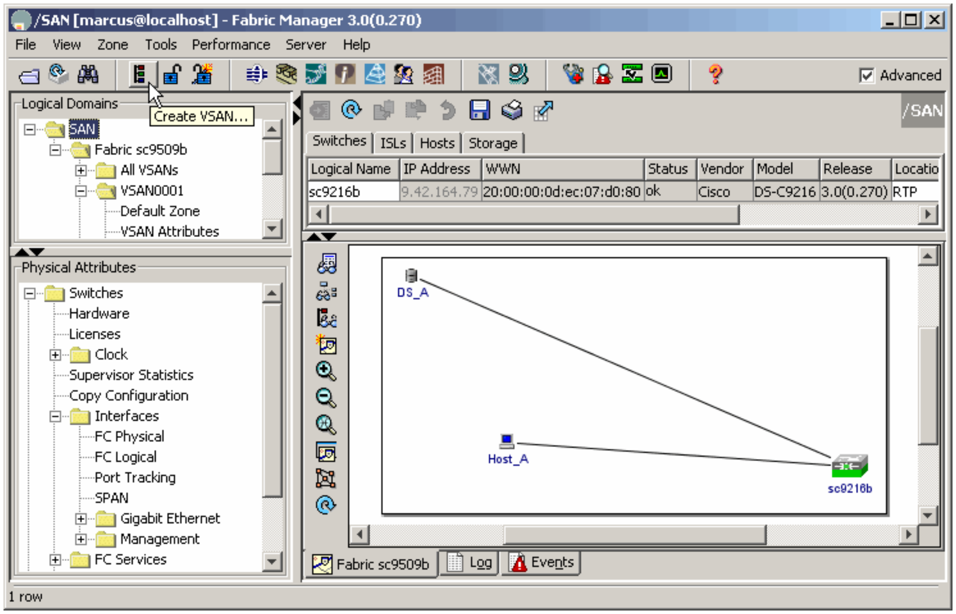
```
sc9216b# config t
Enter configuration commands, one per line.  End with CNTL/Z.
sc9216b(config)# vsan database
sc9216b(config-vsan-db)# vsan 11 interface  fc1/1, fc1/2

sc9216b# sho vsan membership
vsan 1 interfaces:
        fc1/3   fc1/4   fc1/5   fc1/6   fc1/7   fc1/8   fc1/9   fc1/10
        fc1/11  fc1/12  fc1/13  fc1/14  fc1/15  fc1/16  fc2/1   fc2/2
        fc2/3   fc2/4   fc2/5   fc2/6   fc2/7   fc2/8   fc2/9   fc2/10
        fc2/11  fc2/12  fc2/13  fc2/14  fc2/15  fc2/16  fc2/17  fc2/18
        fc2/19  fc2/20  fc2/21  fc2/22  fc2/23  fc2/24  fc2/25  fc2/26
        fc2/27  fc2/28  fc2/29  fc2/30  fc2/31  fc2/32

vsan 11 interfaces:
        fc1/1   fc1/2

vsan 4094(isolated_vsan) interfaces:
```

Note: When assigning port membership to a VSAN, the port is removed from its previously membership, since a port can only be part of one VSAN at a time.

Creating a VSAN using the GUI

Next we perform the same task using the Fabric Manager interface.

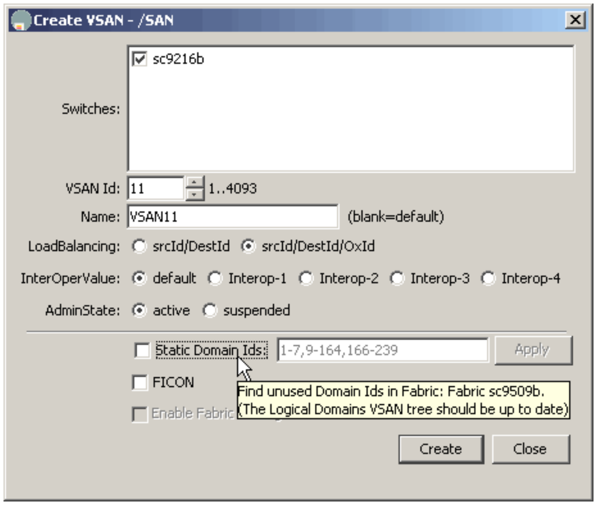
First we click the **Create VSAN** icon as shown in Figure 4-46.


/SAN [marcus@localhost] - Fabric Manager 3.0(0.270)
File View Zone Tools Performance Server Help
☑ Advanced
Create VSAN...
Logical Domains
SAN
Fabric sc9509b
All VSANs
VSAN0001
Default Zone
VSAN Attributes
Physical Attributes
Switches
Hardware
Licenses
Clock
Supervisor Statistics
Copy Configuration
Interfaces
FC Physical
FC Logical
Port Tracking
SPAN
Gigabit Ethernet
Management
FC Services
/SAN
Switches
ISLs
Hosts
Storage
DS_A
Host_A
sc9216b
Fabric sc9509b
Log
Events
1 row

Logical Name	IP Address	WWN	Status	Vendor	Model	Release	Locatio
sc9216b	9.42.164.79	20:00:00:0d:ec:07:d0:80	ok	Cisco	DS-C9216	3.0(0.270)	RTP

Figure 4-46 Creating a VSAN

In the Create VSAN window we specify the VSAN id name and load balancing and interop properties and whether the VSAN should be active or suspended. To enforce static domain ids, we can check mark the **Static Domain Ids** box, as shown in Figure 4-47.



Create VSAN - /SAN

Switches: ☑ sc9216b

VSAN Id: 11 1..4093

Name: VSAN11 (blank=default)

LoadBalancing: ○ srcId/DestId ● srcId/DestId/OxId

InterOperValue: ● default ○ Interop-1 ○ Interop-2 ○ Interop-3 ○ Interop-4

AdminState: ● active ○ suspended

☐ Static Domain Ids: 1-7,9-164,166-239

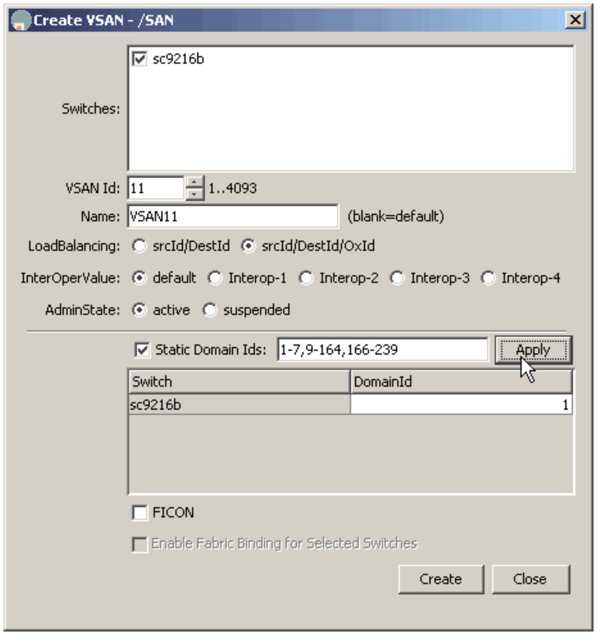
☐ FICON

☐ Enable Fabric

Find unused Domain Ids in Fabric: Fabric sc9509b.
(The Logical Domains VSAN tree should be up to date)

Figure 4-47 Assigning VSAN id and name

We want to use static domain ids, so we check mark this box and click **Apply** to get a static domain id assigned on the switch as shown in Figure 4-48, then click **Create** to create the VSAN.



Create VSAN - /SAN

Switches: ☑ sc9216b

VSAN Id: 11 1..4093

Name: VSAN11 (blank=default)

LoadBalancing: ○ srcId/DestId ● srcId/DestId/OxId

InterOperValue: ● default ○ Interop-1 ○ Interop-2 ○ Interop-3 ○ Interop-4

AdminState: ● active ○ suspended

☑ Static Domain Ids: 1-7,9-164,166-239

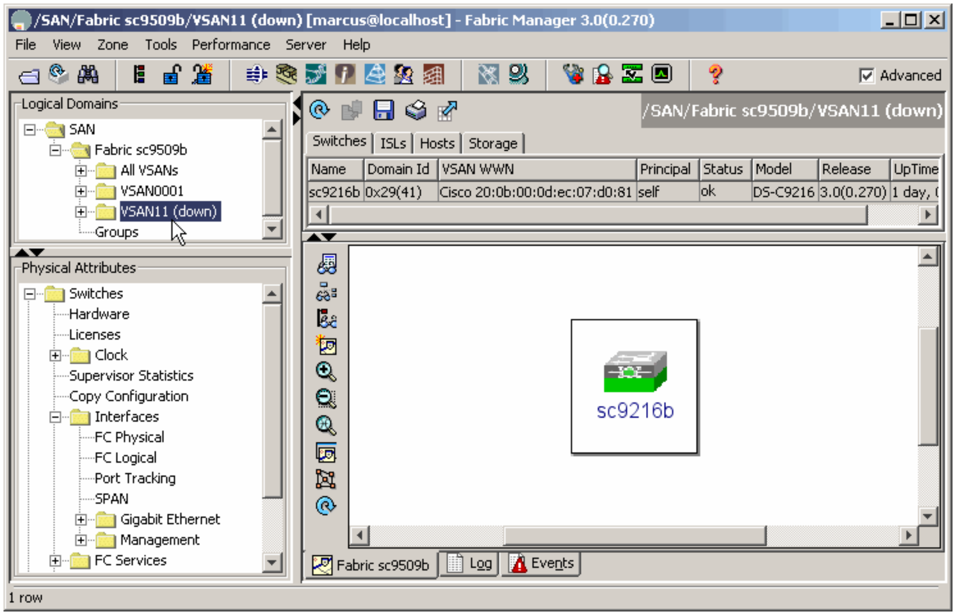
Switch	DomainId
sc9216b	1

☐ FICON

☐ Enable Fabric Binding for Selected Switches

Figure 4-48 Applying static domains

The VSAN has now been created and it appears in Fabric Manager. As shown in Figure 4-49, the VSAN is down, since we have not yet assigned any ports to the VSAN, thus there are no active ports in the VSAN.

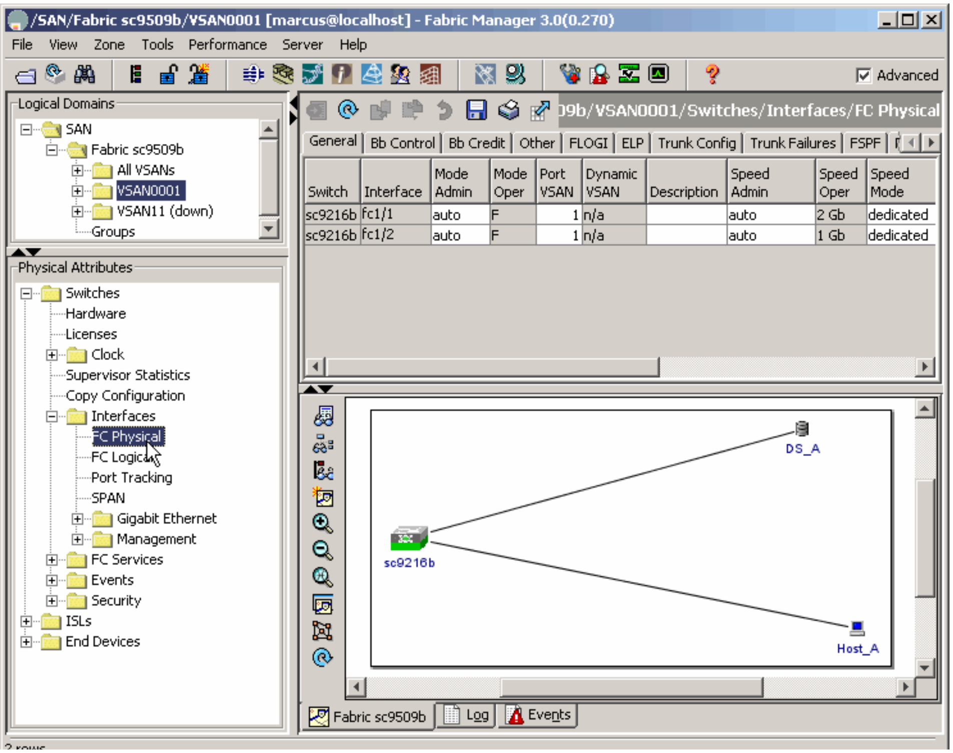

/SAN/Fabric sc9509b/VSAN11 (down) [marcus@localhost] - Fabric Manager 3.0(0.270)
File
View
Zone
Tools
Performance
Server
Help
☑ Advanced
Logical Domains
SAN
Fabric sc9509b
All VSANs
VSAN0001
VSAN11 (down)
Groups
Physical Attributes
Switches
Hardware
Licenses
Clock
Supervisor Statistics
Copy Configuration
Interfaces
FC Physical
FC Logical
Port Tracking
SPAN
Gigabit Ethernet
Management
FC Services
/SAN/Fabric sc9509b/VSAN11 (down)
Switches
ISLs
Hosts
Storage
sc9216b
Fabric sc9509b
Log
Events
1 row

Name	Domain Id	VSAN WWN	Principal	Status	Model	Release	UpTime
sc9216b	0x29(41)	Cisco 20:0b:00:0d:ec:07:d0:81	self	ok	DS-C9216	3.0(0.270)	1 day,

Figure 4-49 VSAN is created -VSAN is down while empty

Assigning ports to a VSAN

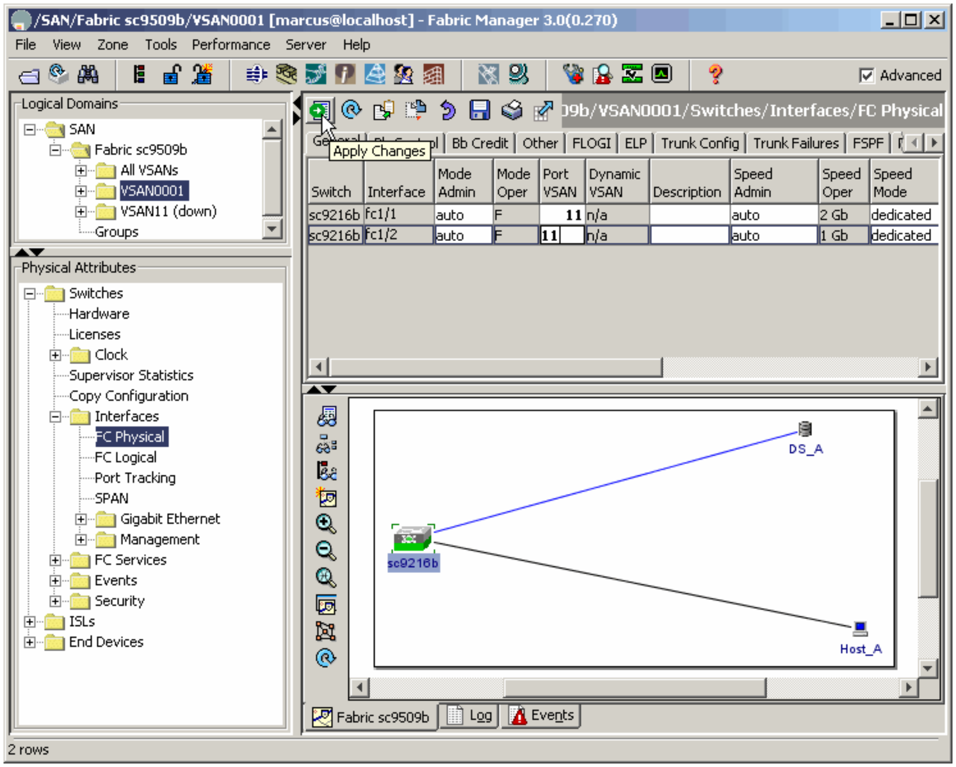
Since our host and device is already connected to the switch, we highlight **FC Interfaces** in VSAN001 to list the ports we want to assign to the VSAN we have created, as shown in Figure 4-50.


/SAN/Fabric sc9509b/VSAN0001 [marcus@localhost] - Fabric Manager 3.0(0.270)
File View Zone Tools Performance Server Help
☑ Advanced
Logical Domains
SAN
Fabric sc9509b
All VSANs
VSAN0001
VSAN11 (down)
Groups
Physical Attributes
Switches
Hardware
Licenses
Clock
Supervisor Statistics
Copy Configuration
Interfaces
FC Physical
FC Logical
Port Tracking
SPAN
Gigabit Ethernet
Management
FC Services
Events
Security
ISLs
End Devices
09b/VSAN0001/Switches/Interfaces/FC Physical
General
Bb Control
Bb Credit
Other
FLOGI
ELP
Trunk Config
Trunk Failures
FSPF
DS_A
sc9216b
Host_A
Fabric sc9509b
Log
Events
2 rows

Switch	Interface	Mode Admin	Mode Oper	Port VSAN	Dynamic VSAN	Description	Speed Admin	Speed Oper	Speed Mode
sc9216b	fc1/1	auto	F	1	n/a		auto	2 Gb	dedicated
sc9216b	fc1/2	auto	F	1	n/a		auto	1 Gb	dedicated

Figure 4-50 Listing devices in VSAN1

We then double-click the *Port VSAN* cell and change the VSAN id to the VSAN id of the VSAN we want to assign the port to, and subsequently click the **Apply Changes** icon to save the changes, as shown in Figure 4-51.



File
View
Zone
Tools
Performance
Server
Help
Advanced
Logical Domains
SAN
Fabric sc9509b
All VSANs
VSAN0001
VSAN11 (down)
Groups
Physical Attributes
Switches
Hardware
Licenses
Clock
Supervisor Statistics
Copy Configuration
Interfaces
FC Physical
FC Logical
Port Tracking
SPAN
Gigabit Ethernet
Management
FC Services
Events
Security
ISLs
End Devices
Apply Changes
Bb Credit
Other
FLOGI
ELP
Trunk Config
Trunk Failures
FSPF
DS_A
sc9216b
Host_A
Fabric sc9509b
Log
Events

/SAN/Fabric sc9509b/VSAN0001 [marcus@localhost] - Fabric Manager 3.0(0.270)

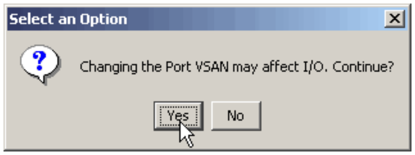
09b/VSAN0001/Switches/Interfaces/FC Physical

Switch	Interface	Mode Admin	Mode Oper	Port VSAN	Dynamic VSAN	Description	Speed Admin	Speed Oper	Speed Mode
sc9216b	fc1/1	auto	F	11	n/a		auto	2 Gb	dedicated
sc9216b	fc1/2	auto	F	11	n/a		auto	1 Gb	dedicated

2 rows

Figure 4-51 Changing the VSAN id for a port to assign it to the VSAN

We are presented with a warning that changing the Port VSAN might be disruptive to IO on the port, and we confirm that we want to perform the change, as shown in Figure 4-52.

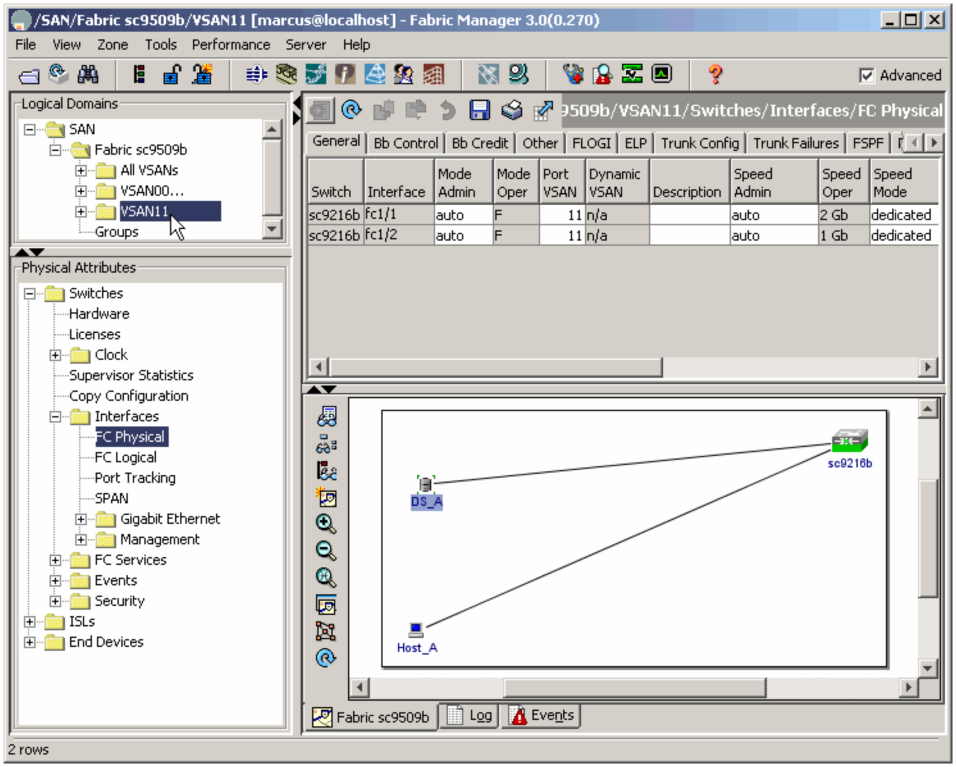


Select an Option

Changing the Port VSAN may affect I/O. Continue?

Figure 4-52 Confirm to change the Port VSAN

When this is completed, we list the ports in our VSAN11 as shown in Figure 4-53, and the VSAN is now up, since active ports are present in the VSAN.


/SAN/Fabric sc9509b/VSAN11 [marcus@localhost] - Fabric Manager 3.0(0.270)
File View Zone Tools Performance Server Help
☑ Advanced
Logical Domains
SAN
Fabric sc9509b
All VSANs
VSAN00...
VSAN11
Groups
Physical Attributes
Switches
Hardware
Licenses
Clock
Supervisor Statistics
Copy Configuration
Interfaces
FC Physical
FC Logical
Port Tracking
SPAN
Gigabit Ethernet
Management
FC Services
Events
Security
ISLs
End Devices
9509b/VSAN11/Switches/Interfaces/FC Physical
General
Bb Control
Bb Credit
Other
FLOGI
ELP
Trunk Config
Trunk Failures
FSPF
sc9216b
DS_A
Host_A
Fabric sc9509b
Log
Events
2 rows

Switch	Interface	Mode Admin	Mode Oper	Port VSAN	Dynamic VSAN	Description	Speed Admin	Speed Oper	Speed Mode
sc9216b	fc1/1	auto	F	11	n/a		auto	2 Gb	dedicated
sc9216b	fc1/2	auto	F	11	n/a		auto	1 Gb	dedicated

Figure 4-53 Listing ports in the our new VSAN

Dynamic VSANs

Port VSAN membership on the switch is assigned on a port-by-port basis. By default each port belongs to the default VSAN.

You can dynamically assign VSAN membership to ports by assigning VSANs based on the device WWN. This method is referred to as the Dynamic Port VSAN Membership (DPVM) feature. DPVM offers flexibility and eliminates the necessity to reconfigure the VSAN to maintain fabric topology when a host or storage device connection is moved between two Cisco MDS switches. It retains the configured VSAN regardless of where a device is connected or moved.

About DPVM

DPVM configurations are based on port world wide name (pWWN) and node world wide name (nWWN) assignments. A DPVM database contains mapping information for each device pWWN/nWWN assignment and the corresponding VSAN. The Cisco SAN-OS software checks the database during a device FLOGI and obtains the required VSAN details.

The pWWN identifies the host or device and the nWWN identifies a node consisting of multiple devices. You can assign any one of these identifiers or any combination of these identifiers to configure DPVM mapping. If you assign a combination, then preference is given to the pWWN. DPVM uses the Cisco Fabric Services (CFS) infrastructure to allow efficient database management and distribution. DPVM uses the application driven, coordinated distribution mode and the fabric-wide distribution scope

DPVM requirements

To use the DPVM feature as designed, be sure to verify the following requirements:

- The interface through which the dynamic device connects to the Cisco MDS 9000 family switch must be configured as an F port.
- The static port VSAN of the F port should be valid (not isolated, not suspended and in existence).
- The dynamic VSAN configured for the device in the DPVM database should be valid (not isolated, not suspended and in existence).

Note: The DPVM feature overrides any existing static port VSAN membership configuration. If the VSAN corresponding to the dynamic port is deleted or suspended, the port is shut down.

Enabling DPVM

To begin configuring the DPVM feature, you must explicitly enable DPVM on the required switches in the fabric. By default, this feature is disabled in all switches in the Cisco MDS 9000 family. The configuration and verification commands for the DPVM feature are only available when DPVM is enabled on a switch. When you disable this feature, all related configurations are automatically discarded.

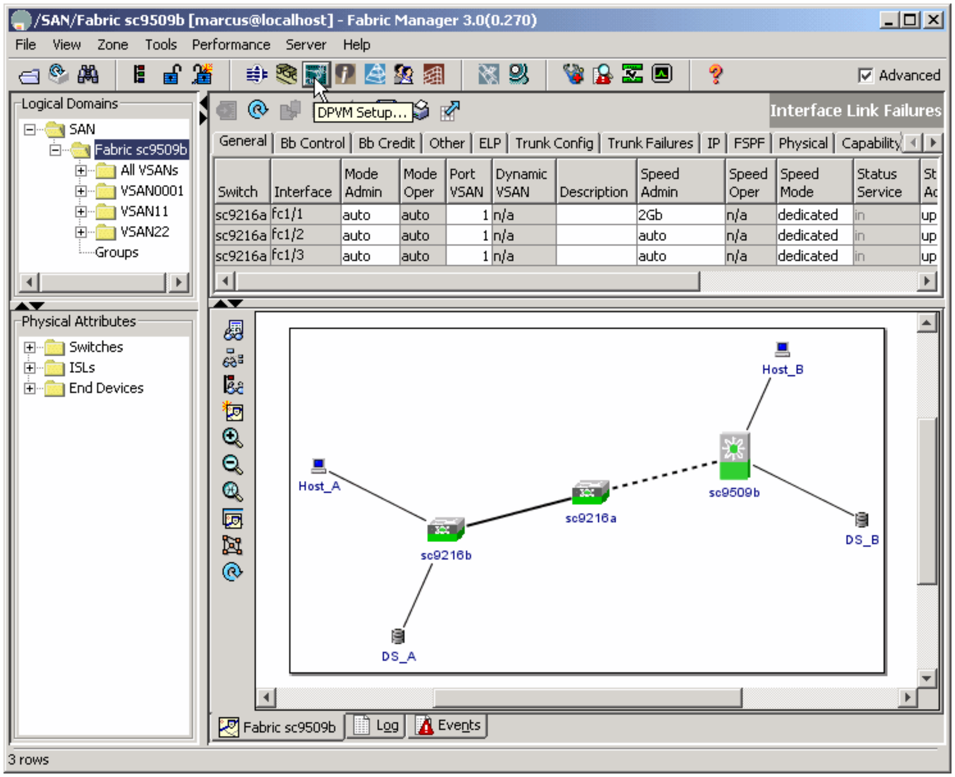
To enable DPVM on any participating switch, follow these steps:

1. `switch# config t`
2. `switch(config)#`

   This enters configuration mode.
3. `switch(config)# dpvm enable`

   This enables DPVM on that switch.

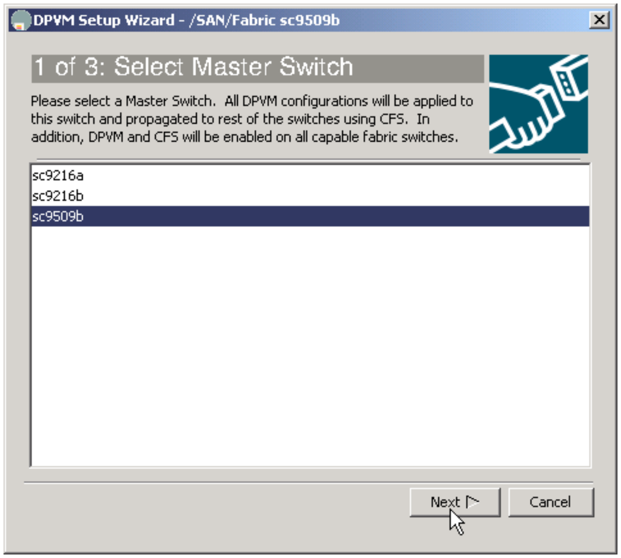
To use DPVM using the GUI, we click the **DPVM icon** as shown in Example 4-54.


/SAN/Fabric sc9509b [marcus@localhost] - Fabric Manager 3.0(0.270)
File
View
Zone
Tools
Performance
Server
Help
☑ Advanced
DPVM Setup...
Interface Link Failures
Logical Domains
SAN
Fabric sc9509b
All VSANs
VSAN0001
VSAN11
VSAN22
Groups
Physical Attributes
Switches
ISLs
End Devices
General
Bb Control
Bb Credit
Other
ELP
Trunk Config
Trunk Failures
IP
FSPF
Physical
Capability
Host_B
Host_A
sc9509b
sc9216a
sc9216b
DS_B
DS_A
Fabric sc9509b
Log
Events
3 rows

Switch	Interface	Mode Admin	Mode Oper	Port VSAN	Dynamic VSAN	Description	Speed Admin	Speed Oper	Speed Mode	Status Service	St Ac
sc9216a	fc1/1	auto	auto	1	n/a		2Gb	n/a	dedicated	in	up
sc9216a	fc1/2	auto	auto	1	n/a		auto	n/a	dedicated	in	up
sc9216a	fc1/3	auto	auto	1	n/a		auto	n/a	dedicated	in	up

Figure 4-54 Launching the DPVM wizard

We select the switch we want to be the master DPVM switch and click **Next** as shown in Figure 4-55.


DPVM Setup Wizard - /SAN/Fabric sc9509b

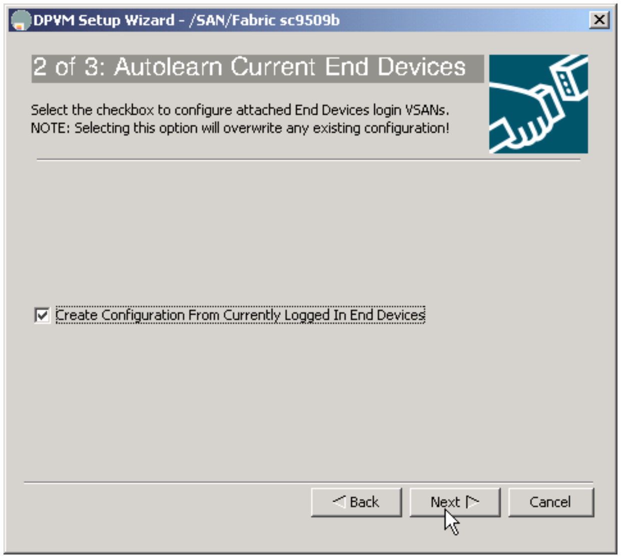
1 of 3: Select Master Switch

Please select a Master Switch. All DPVM configurations will be applied to this switch and propagated to rest of the switches using CFS. In addition, DPVM and CFS will be enabled on all capable fabric switches.

sc9216a
sc9216b
sc9509b

Figure 4-55 Selecting the master switch

We select to create the configuration from already logged in devices as shown in Figure 4-56.


DPVM Setup Wizard - /SAN/Fabric sc9509b

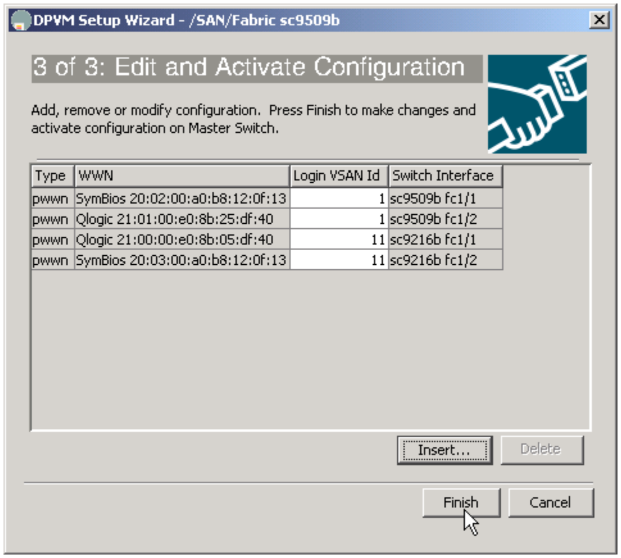
2 of 3: Autolearn Current End Devices

Select the checkbox to configure attached End Devices login VSANs.
NOTE: Selecting this option will overwrite any existing configuration!

☑ Create Configuration From Currently Logged In End Devices

Figure 4-56 Creating configuration from end devices currently logged in

As shown in Example 4-57, we click **Finish** to activate the configuration.



3 of 3: Edit and Activate Configuration

Add, remove or modify configuration. Press Finish to make changes and activate configuration on Master Switch.

Type	WWN	Login VSAN Id	Switch Interface
pwwn	SymBios 20:02:00:a0:b8:12:0f:13	1	sc9509b fc1/1
pwwn	Qlogic 21:01:00:e0:8b:25:df:40	1	sc9509b fc1/2
pwwn	Qlogic 21:00:00:e0:8b:05:df:40	11	sc9216b fc1/1
pwwn	SymBios 20:03:00:a0:b8:12:0f:13	11	sc9216b fc1/2

Figure 4-57 Edit and activate configuration

4.6.9 Zoning

The Cisco MDS 9000 family zoning can be administrated from any switch in the fabric, and all changes are automatically distributed to all of the switches.

The Cisco MDS 9000 family supports zoning by the following criteria:

- World Wide Port Name (WWPN) — the WWN of the Nx_Port (device) attached to the switch
- Fabric Port WWN (fWWN) — the WWN of the fabric port (port-based zoning)
- FCID — the FCID of the N_Port attached to the switch
- FC alias — the alias used
- Domain ID — where the domain id is the domain id of a switch
- IP address — where the IP address of the device(s) is entered as a 32-byte dotted decimal optionally specifying a subnet mask which includes all addresses in the specified subnet.
- Interface — Switch interface zoning is similar to port zoning and can be defined as a zone member on both a local and remote switch.

To make zone management easier, the Cisco MDS 9000 family supports alias names for practically all of the elements above.

The Cisco MDS 9000 family supports a default zone. All ports and WWNs not assigned to any zone belong to the default zone. If zoning is not activated, all devices belong to the default zone. You can control access between default zone members by default zone policy. This is both a per-switch (defined at setup) and a per-VSAN setting. The default is deny, but can be changed using the config command **`zone default-zone permit`**. In Example 4-16 we set the default zone policy to permit for VSAN11.

Example 4-16 Setting the default zone policy for a VSAN

```
h3csco9509# config
h3csco9509(config)# zone default-zone permit vsan 11
```

The Cisco MDS 9000 family supports both soft and hard zoning, the difference in soft and hard zone enforcement are described below.

Soft zoning

In soft zoning, zoning restrictions are applied during the interaction between the name server and the end device.

Hard zoning

In hard zoning, the zoning is enforced for each frame sent by an Nx_Port as the frame enters the switch. This prevents any unauthorized access at all times. The enforcement is done by the switch hardware at wire speed.

4.6.10 Zoning using the CLI

When creating zoning, we recommend that you use aliases, since this eases administration and troubleshooting, especially when your SAN environment increases in size.

Alias

Alias members can be assigned to an alias based on FC ID, fabric port WWN, or WWPN.

Next we list the entries in the name server and create the alias Host_A assigning the FC ID of the port the host is attached to, as shown in Example 4-17.

Example 4-17 Creating an alias and assigning a member based on FC ID

```
sc9216b# sho fcns database

VSAN 11:
--------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------
```

```
0x290000    N     21:00:00:e0:8b:05:df:40 (Qlogic)       scsi-fcp:init
0x290100    N     20:03:00:a0:b8:12:0f:13 (SymBios)      scsi-fcp:both
Total number of entries = 2

sc9216b# config t
Enter configuration commands, one per line.  End with CNTL/Z.
sc9216b(config)# fcalias name Host_A vsan 11
sc9216b(config-fcalias)# member fcid 0x290000
sc9216b(config-fcalias)# end

sc9216b# sho fcalias
fcalias name Host_A vsan 11
  fcid 0x290000
```

In the following coding, we create the alias DS_A assigning the WWPN of the disk subsystem, and finally list the defined aliases, as shown in Example 4-18.

Example 4-18   Creating an alias and assigning a member based on WWPN

```
sc9216b# config t
Enter configuration commands, one per line.  End with CNTL/Z.
sc9216b(config)# fcalias name DS_A vsan 11
sc9216b(config-fcalias)# member pwwn 20:03:00:a0:b8:12:0f:13
sc9216b(config-fcalias)# end

sc9216b# sho fcalias
fcalias name DS_A vsan 11
  pwwn 20:03:00:a0:b8:12:0f:13

fcalias name Host_A vsan 11
  fcid 0x290000
```

Zones

When creating a zone, we recommend zones based on aliases, and in the following coding, we create a zone called *Host_A_to_Disk* for Host_A access to DS_A. As shown in Example 4-19, we create the zone and subsequently list defined zones.

Example 4-19   Creating a zone

```
sc9216b# config t
Enter configuration commands, one per line.  End with CNTL/Z.
sc9216b(config)# zone name Host_A_to_Disk vsan 11
sc9216b(config-zone)# member fcalias Host_A
sc9216b(config-zone)# member fcalias DS_A
sc9216b(config-zone)# end
```

```
sc9216b# sho zone
zone name Host_A_to_Disk vsan 11
  fcalias name Host_A vsan 11
    fcid 0x290000

  fcalias name DS_A vsan 11
    pwwn 20:03:00:a0:b8:12:0f:13
```

For the zone to become active, we must then assign the zone to a zoneset and activate the zoneset.

Zone set

Where a zone is used to specify access control, confining the specified members in a zone, Zone sets are used to group zones and to enforce the access control defined by each zone when the zone set is activated.

To create a zone set, we specify the name, VSAN, and members of the zoneset. In Example 4-20 we create the zoneset *ITSO_1* in *VSAN 11* and add the zone *Host_A_to_Disk*, and subsequently list the zone set.

Example 4-20 Creating a zone set

```
sc9216b# sho zoneset
Zoneset not present

sc9216b# config t
Enter configuration commands, one per line.  End with CNTL/Z.
sc9216b(config)# zoneset name ITSO_1 vsan 11
sc9216b(config-zoneset)# member Host_A_to_Disk
sc9216b(config-zoneset)# end

sc9216b# sho zoneset
zoneset name ITSO_1 vsan 11
  zone name Host_A_to_Disk vsan 11
    fcalias name Host_A vsan 11
      fcid 0x290000

    fcalias name DS_A vsan 11
      pwwn 20:03:00:a0:b8:12:0f:13
```

Before a zone set is enforced, it must activated. To activate a zone set, we specify the zone set and the VSAN. In Example 4-21 we first list active zone sets, then we activate the zone set ITSO_1 in VSAN11, and subsequently list active zone sets.

Example 4-21 Activating a zoneset

```
sc9216b# sho zoneset active
Zoneset not present

sc9216b# config t
Enter configuration commands, one per line.  End with CNTL/Z.
sc9216b(config)# zoneset activate name ITSO_1 vsan 11
Zoning database analysis vsan 11
Formatted database size: < 1 Kb ( < 1% usage)
 Active zoneset
  Ave. zone members: 2
  Formattted size: < 1 Kb
 Full zoning database
  Database not available
Zoneset activation initiated. check zone status

sc9216b# sho zoneset active
zoneset name ITSO_1 vsan 11
  zone name Host_A_to_Disk vsan 11
  * fcid 0x290000
  * fcid 0x290100 [pwwn 20:03:00:a0:b8:12:0f:13]
```

When working with zone sets, it is crucial to understand that while you can create multiple zone sets (and zones can be members of multiple zone sets) — only ***one*** zone set can be active at any given time (for each VSAN).

When creating a zone set, the zoneset becomes part of the full zone set, and when activating a zone set, a copy of the zone set from the full zone set is activated and the member zones become active.

Although the active zone set cannot be modified, we can modify the full zone set, even a zoneset with the same name. However, modifications only take effect when reactivated.

While the active zone set, it is automatically stored in the persistent configuration. It is not necessary to copy the running-config to the startup-config, though changes to inactive zone sets are not automatically saved to the startup-config, unless you perform this by issuing the **`copy running-config startup config`** command.

4.6.11 Zoning using the GUI

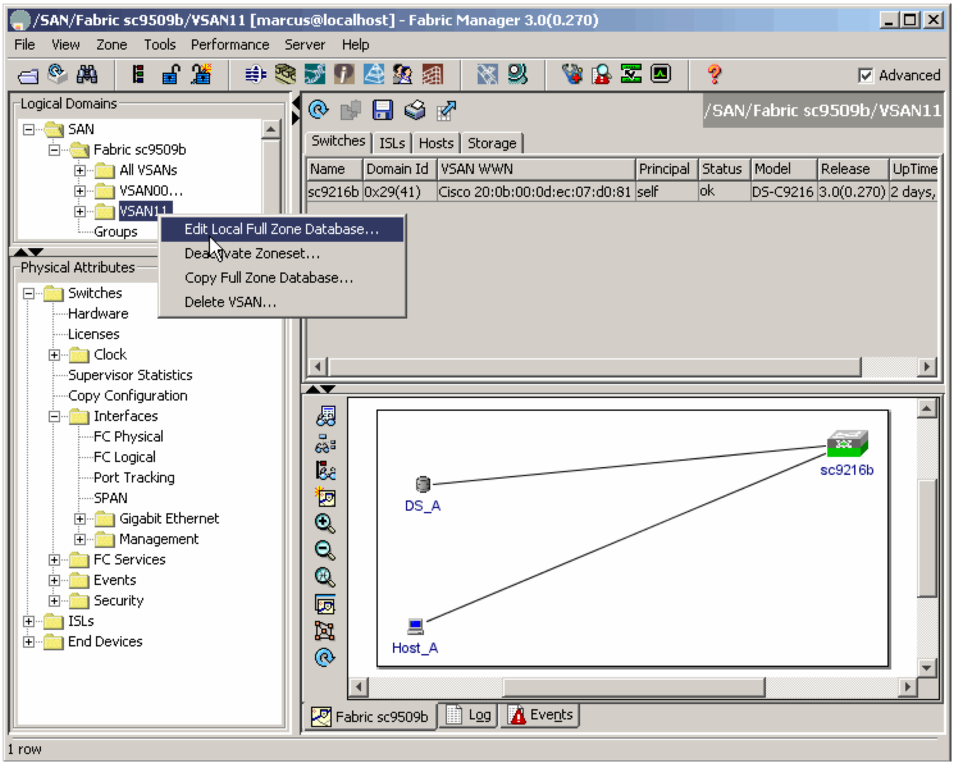
When creating zoning, we recommend that you use aliases, since this eases administration and troubleshooting, especially when your SAN environment increases in size.

> **Note:** In the following topics, we go through the examples mainly by right-clicking the objects we want to alter. When you get more familiar with the GUI, you will see that there are multiple ways to perform the same task, and that drag-and-drop is also available for many tasks.

Alias

Alias members can be assigned to an alias based on FC ID, fabric port WWN, or WWPN.

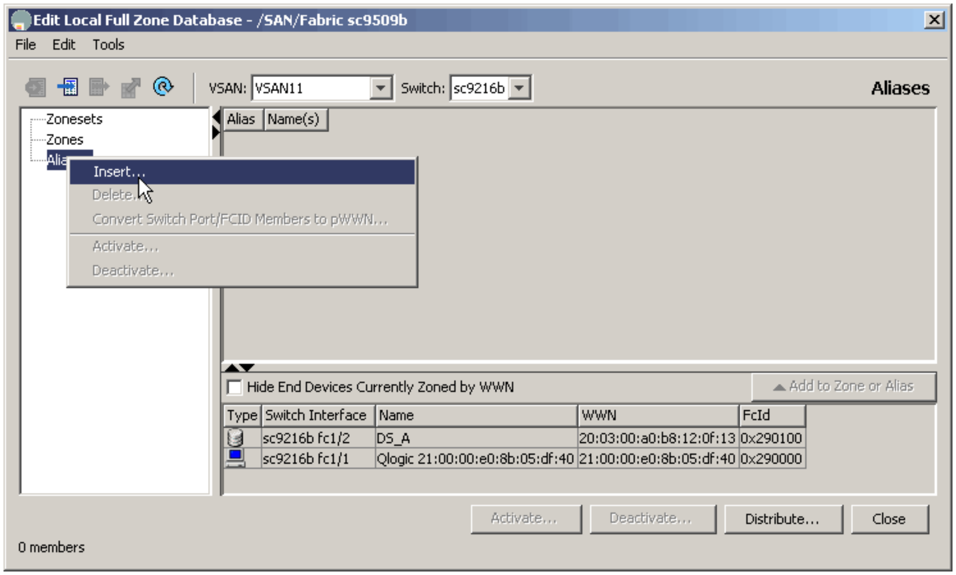
In the following example, we create the alias DS_A assigning the WWPN of the disk subsystem. As shown in Figure 4-58, we right-click the VSAN to select to edit the full zone set.


/SAN/Fabric sc9509b/VSAN11 [marcus@localhost] - Fabric Manager 3.0(0.270)
File
View
Zone
Tools
Performance
Server
Help
☑ Advanced
Logical Domains
SAN
Fabric sc9509b
All VSANs
VSAN00...
VSAN11
Groups
Edit Local Full Zone Database...
Deactivate Zoneset...
Copy Full Zone Database...
Delete VSAN...
Physical Attributes
Switches
Hardware
Licenses
Clock
Supervisor Statistics
Copy Configuration
Interfaces
FC Physical
FC Logical
Port Tracking
SPAN
Gigabit Ethernet
Management
FC Services
Events
Security
ISLs
End Devices
/SAN/Fabric sc9509b/VSAN11
Switches
ISLs
Hosts
Storage
DS_A
sc9216b
Host_A
Fabric sc9509b
Log
Events
1 row

Name	Domain Id	VSAN WWN	Principal	Status	Model	Release	UpTime
sc9216b	0x29(41)	Cisco 20:0b:00:0d:ec:07:d0:81	self	ok	DS-C9216	3.0(0.270)	2 days,

Figure 4-58 Edit full zone set

In the edit full zone set database, we right-click **Aliases** to insert a new alias as shown in Figure 4-59.


Edit Local Full Zone Database - /SAN/Fabric sc9509b
File
Edit
Tools
Aliases
Zonesets
Zones
Alia
Insert...
Delete...
Convert Switch Port/FCID Members to pWWN...
Activate...
Deactivate...
Alias
Name(s)
Add to Zone or Alias
Activate...
Deactivate...
Distribute...
Close

VSAN: VSAN11 Switch: sc9216b

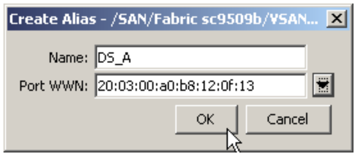
☐ Hide End Devices Currently Zoned by WWN

Type	Switch Interface	Name	WWN	FcId
	sc9216b fc1/2	DS_A	20:03:00:a0:b8:12:0f:13	0x290100
	sc9216b fc1/1	Qlogic 21:00:00:e0:8b:05:df:40	21:00:00:e0:8b:05:df:40	0x290000

0 members

Figure 4-59 Inserting an alias

In the Create Alias window, we name the alias, and assign the WWPN (selected from the dropdown menu) and click **OK**, as shown in Figure 4-60.

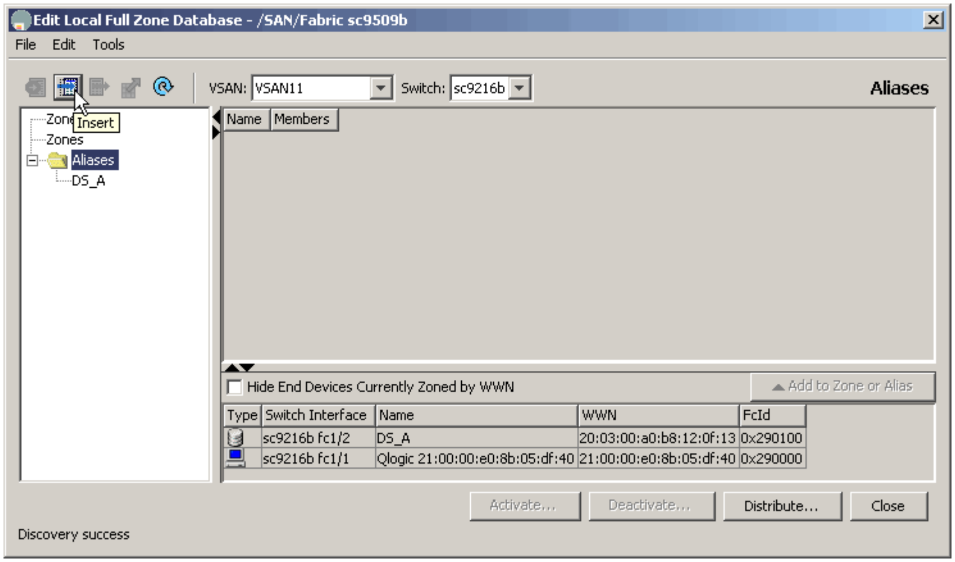

Create Alias - /SAN/Fabric sc9509b/VSAN...
OK
Cancel

Name: DS_A
Port WWN: 20:03:00:a0:b8:12:0f:13

Figure 4-60 Creating alias based on WWPN

Then we create the alias Host_A, assigning the FC ID of the port the host is attached to as the member.

As shown in Figure 4-61, we click the **Insert** icon to enter a new alias.


Edit Local Full Zone Database - /SAN/Fabric sc9509b
File
Edit
Tools
Insert
Zone
Zones
Aliases
DS_A
Aliases
Name
Members
Hide End Devices Currently Zoned by WWN
Add to Zone or Alias
Activate...
Deactivate...
Distribute...
Close

VSAN: VSAN11

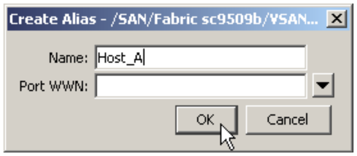
Switch: sc9216b

Type	Switch Interface	Name	WWN	FcId
	sc9216b fc1/2	DS_A	20:03:00:a0:b8:12:0f:13	0x290100
	sc9216b fc1/1	Qlogic 21:00:00:e0:8b:05:df:40	21:00:00:e0:8b:05:df:40	0x290000

Discovery success

Figure 4-61 Clicking the insert icon

We name the new alias Host_A and click **OK** to create the empty alias, as shown in Figure 4-62.

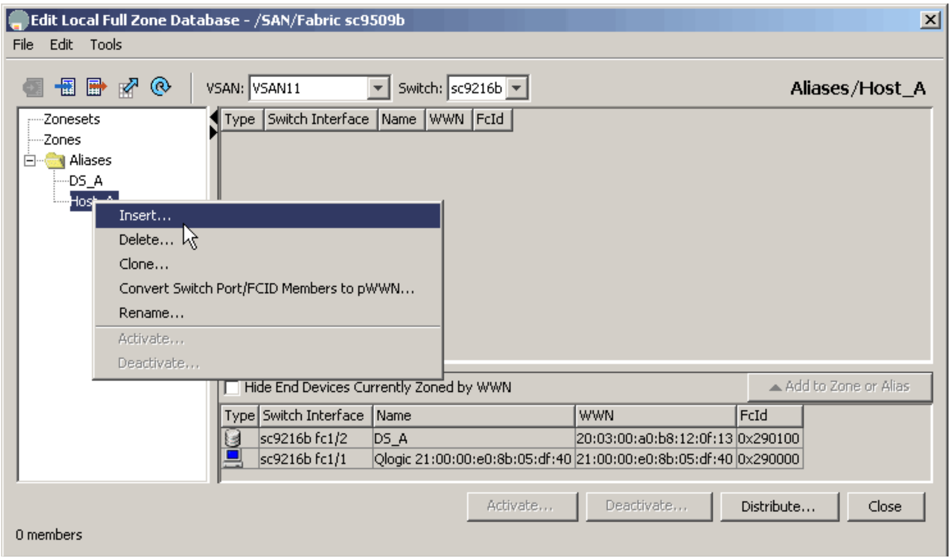

Create Alias - /SAN/Fabric sc9509b/VSAN...
OK
Cancel

Name: Host_A

Port WWN:

Figure 4-62 Defining an empty alias

We right-click the created **alias Host_A** and select **Insert...** as shown in Figure 4-63, in order to modify the alias.


Edit Local Full Zone Database - /SAN/Fabric sc9509b
File
Edit
Tools
Aliases/Host_A
Zonesets
Zones
Aliases
DS_A
Host_A
Insert...
Delete...
Clone...
Convert Switch Port/FCID Members to pWWN...
Rename...
Activate...
Deactivate...
Type
Switch Interface
Name
WWN
FcId
Add to Zone or Alias
Activate...
Deactivate...
Distribute...
Close

VSAN: VSAN11

Switch: sc9216b

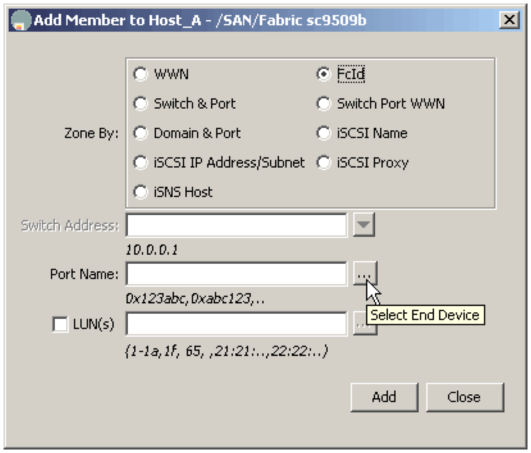
☐ Hide End Devices Currently Zoned by WWN

Type	Switch Interface	Name	WWN	FcId
	sc9216b fc1/2	DS_A	20:03:00:a0:b8:12:0f:13	0x290100
	sc9216b fc1/1	Qlogic 21:00:00:e0:8b:05:df:40	21:00:00:e0:8b:05:df:40	0x290000

0 members

Figure 4-63 Selecting the alias to be modified

To define the alias member, we mark the FCID and click the **Select End Device** icon as shown in Figure 4-64.


Add Member to Host_A - /SAN/Fabric sc9509b
Select End Device
Add
Close

Zone By:

○ WWN ● FcId

○ Switch & Port ○ Switch Port WWN

○ Domain & Port ○ iSCSI Name

○ iSCSI IP Address/Subnet ○ iSCSI Proxy

○ iSNS Host

Switch Address:

10.0.0.1

Port Name:

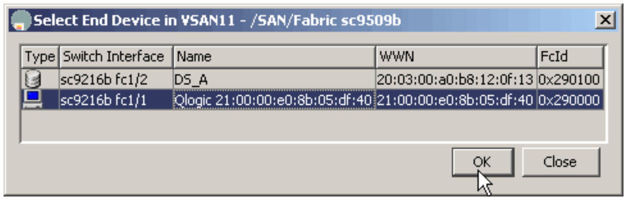
0x123abc,0xabc123,..

☐ LUN(s)

{1-1a,1f, 65, ,21:21:..,22:22:..}

Figure 4-64 Select membership type and end device

We highlight the desired end device and click **OK** as shown in Figure 4-65.

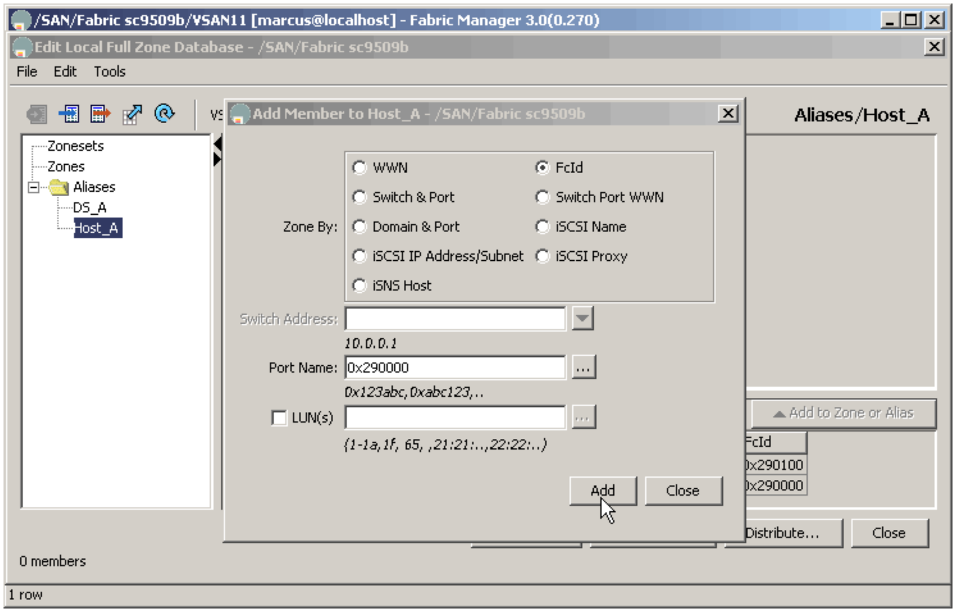


Select End Device in VSAN11 - /SAN/Fabric sc9509b

Type	Switch Interface	Name	WWN	FcId
	sc9216b fc1/2	DS_A	20:03:00:a0:b8:12:0f:13	0x290100
	sc9216b fc1/1	Qlogic 21:00:00:e0:8b:05:df:40	21:00:00:e0:8b:05:df:40	0x290000

Figure 4-65 Selecting the end device

We have now defined the properties for the alias member Host_A, and click **Add** as shown in Figure 4-66.



/SAN/Fabric sc9509b/VSAN11 [marcus@localhost] - Fabric Manager 3.0(0.270)

Edit Local Full Zone Database - /SAN/Fabric sc9509b

Add Member to Host_A - /SAN/Fabric sc9509b

Zone By: ● FcId

Switch Address:

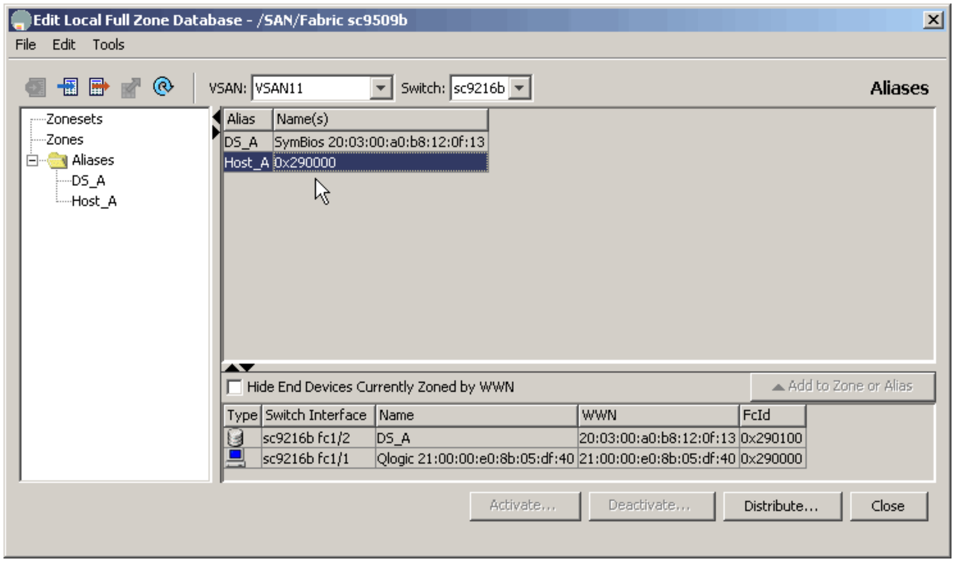
Port Name: 0x290000

☐ LUN(s)

File
Edit
Tools
Zonesets
Zones
Aliases
DS_A
Host_A
Aliases/Host_A
○ WWN
● FcId
○ Switch & Port
○ Switch Port WWN
○ Domain & Port
○ iSCSI Name
○ iSCSI IP Address/Subnet
○ iSCSI Proxy
○ iSNS Host
10.0.0.1
0x123abc, 0xabc123,..
(1-1a, 1f, 65, ,21:21:..,22:22:..)
Add
Close
Add to Zone or Alias
FcId
x290100
x290000
Distribute...
Close
0 members
1 row

Figure 4-66 Add the alias member

Finally we list the defined aliases and verify that they are created as configured, as shown in Figure 4-67.


Edit Local Full Zone Database - /SAN/Fabric sc9509b
File
Edit
Tools
Aliases
Zonesets
Zones
Aliases
DS_A
Host_A
Hide End Devices Currently Zoned by WWN
Add to Zone or Alias
Activate...
Deactivate...
Distribute...
Close

VSAN: VSAN11 Switch: sc9216b

Alias	Name(s)
DS_A	SymBios 20:03:00:a0:b8:12:0f:13
Host_A	0x290000

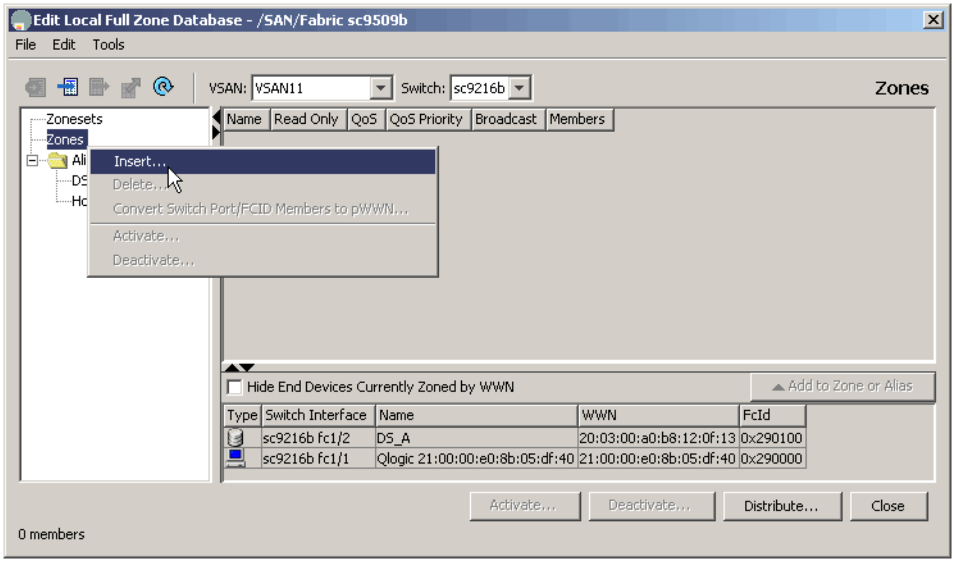
☐ Hide End Devices Currently Zoned by WWN

Type	Switch Interface	Name	WWN	FcId
	sc9216b fc1/2	DS_A	20:03:00:a0:b8:12:0f:13	0x290100
	sc9216b fc1/1	Qlogic 21:00:00:e0:8b:05:df:40	21:00:00:e0:8b:05:df:40	0x290000

Figure 4-67 Listing defined aliases

Zones

To create a zone we right-click **Zones** to insert a new zone as shown in Figure 4-68.


Edit Local Full Zone Database - /SAN/Fabric sc9509b
File
Edit
Tools
Zones
Zonesets
Zones
Ali
DS
Hc
Insert...
Delete...
Convert Switch Port/FCID Members to pWWN...
Activate...
Deactivate...
Name
Read Only
QoS
QoS Priority
Broadcast
Members
Hide End Devices Currently Zoned by WWN
Add to Zone or Alias
Activate...
Deactivate...
Distribute...
Close

VSAN: VSAN11 Switch: sc9216b

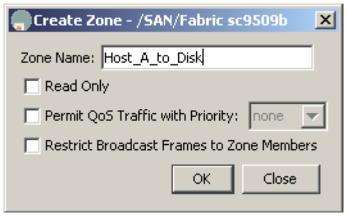
☐ Hide End Devices Currently Zoned by WWN

Type	Switch Interface	Name	WWN	FcId
	sc9216b fc1/2	DS_A	20:03:00:a0:b8:12:0f:13	0x290100
	sc9216b fc1/1	Qlogic 21:00:00:e0:8b:05:df:40	21:00:00:e0:8b:05:df:40	0x290000

0 members

Figure 4-68 Creating a new zone

We name the new zone and can apply specific properties for the zone such as *Read Only*, *QoS* and *broadcast frame restrictions* as shown in Figure 4-69. We name the zone *Host_A_to_Disk* with default zone properties and click **OK**.


Create Zone - /SAN/Fabric sc9509b
OK
Close

Zone Name: Host_A_to_Disk

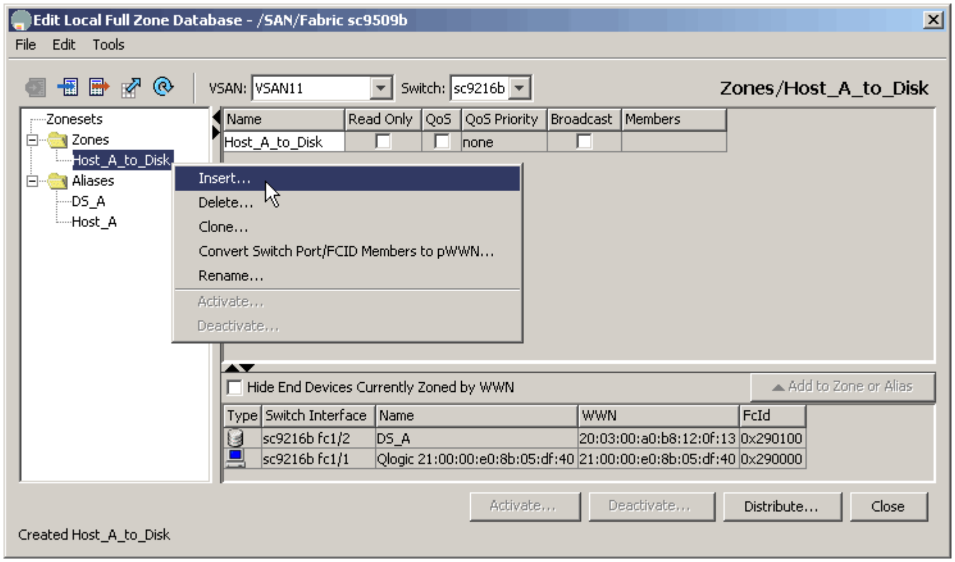
☐ Read Only

☐ Permit QoS Traffic with Priority: none

☐ Restrict Broadcast Frames to Zone Members

Figure 4-69 Naming the zone

We right-click the created zone, and select **Insert** to define members of the zone as shown in Figure 4-70.


Edit Local Full Zone Database - /SAN/Fabric sc9509b
File
Edit
Tools
Zones/Host_A_to_Disk
Zonesets
Zones
Host_A_to_Disk
Aliases
DS_A
Host_A
Insert...
Delete...
Clone...
Convert Switch Port/FCID Members to pWWN...
Rename...
Activate...
Deactivate...
Add to Zone or Alias
Activate...
Deactivate...
Distribute...
Close

VSAN: VSAN11 Switch: sc9216b

Name	Read Only	QoS	QoS Priority	Broadcast	Members
Host_A_to_Disk	☐	☐	none	☐	

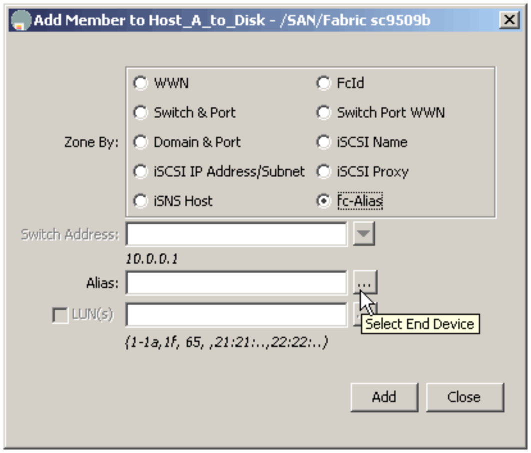
☐ Hide End Devices Currently Zoned by WWN

Type	Switch Interface	Name	WWN	FcId
	sc9216b fc1/2	DS_A	20:03:00:a0:b8:12:0f:13	0x290100
	sc9216b fc1/1	Qlogic 21:00:00:e0:8b:05:df:40	21:00:00:e0:8b:05:df:40	0x290000

Created Host_A_to_Disk

Figure 4-70 Selecting the zone to be modified

We select to add **Fc-Alias** members and click the **Select Devices** icon to list available aliases as shown in Figure 4-71.



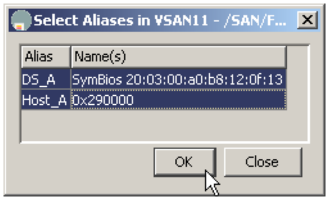
Add Member to Host_A_to_Disk - /SAN/Fabric sc9509b

Zone By:
○ WWN ○ FcId
○ Switch & Port ○ Switch Port WWN
○ Domain & Port ○ iSCSI Name
○ iSCSI IP Address/Subnet ○ iSCSI Proxy
○ iSNS Host ● Fc-Alias

Switch Address:
10.0.0.1
Alias:
☐ LUN(s)
{1-1a,1f, 65, ,21:21:..,22:22:..}

Figure 4-71 Listing aliases

We select the aliases to be members of the zone and click **OK**, as shown in Figure 4-72.

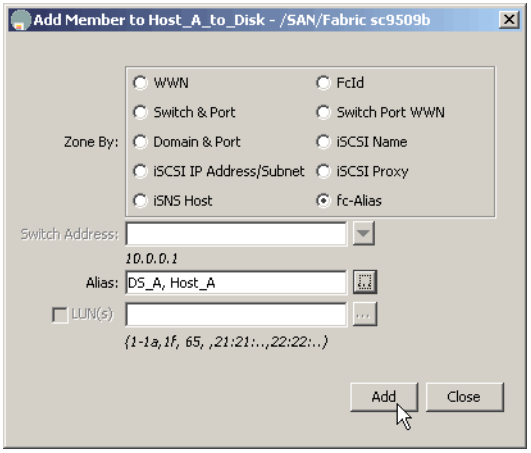


Select Aliases in VSAN11 - /SAN/F...

Alias	Name(s)
DS_A	SymBios 20:03:00:a0:b8:12:0f:13
Host_A	0x290000

Figure 4-72 Selecting end devices

We click **Add** to insert the aliases as members of the zone as shown in Figure 4-73.

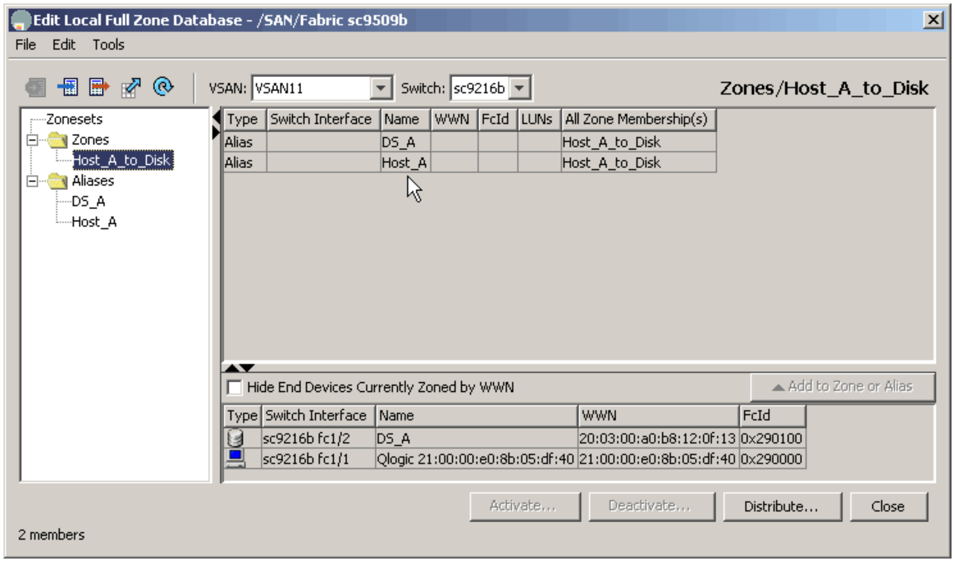

Add Member to Host_A_to_Disk - /SAN/Fabric sc9509b
Add
Close

Zone By:
○ WWN ○ FcId
○ Switch & Port ○ Switch Port WWN
○ Domain & Port ○ iSCSI Name
○ iSCSI IP Address/Subnet ○ iSCSI Proxy
○ iSNS Host ● fc-Alias

Switch Address:
10.0.0.1
Alias: DS_A, Host_A
☐ LUN(s)
(1-1a,1f, 65, ,21:21:..,22:22:..)

Figure 4-73 Adding the devices to the zone

We click the zone *Host_A_to_Disk* to verify the members *Host_A* and *DS_A* as shown in Figure 4-74.


Edit Local Full Zone Database - /SAN/Fabric sc9509b
File
Edit
Tools
Zonesets
Zones
Host_A_to_Disk
Aliases
DS_A
Host_A
Add to Zone or Alias
Activate...
Deactivate...
Distribute...
Close

VSAN: VSAN11 Switch: sc9216b

Zones/Host_A_to_Disk

Type	Switch Interface	Name	WWN	FcId	LUNs	All Zone Membership(s)
Alias		DS_A				Host_A_to_Disk
Alias		Host_A				Host_A_to_Disk

☐ Hide End Devices Currently Zoned by WWN

Type	Switch Interface	Name	WWN	FcId
	sc9216b fc1/2	DS_A	20:03:00:a0:b8:12:0f:13	0x290100
	sc9216b fc1/1	Qlogic 21:00:00:e0:8b:05:df:40	21:00:00:e0:8b:05:df:40	0x290000

2 members

Figure 4-74 Listing the created zone

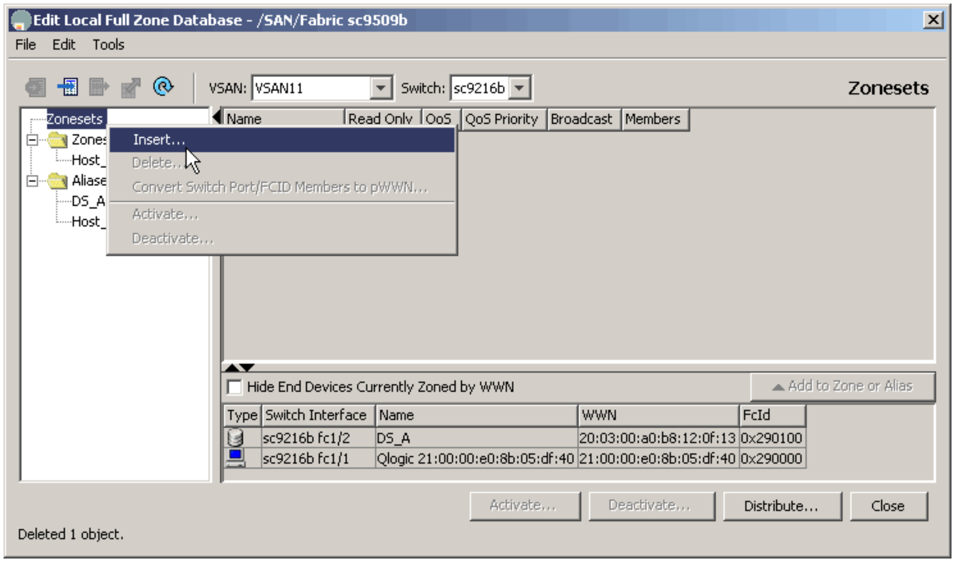
We have now created our zone.

Zone set

Where a zone is used to specify access control, confining the specified members in a zone, zone sets are used to group zones and to enforce the access control defined by each zone when the zone set is activated.

To create a zone set, we specify the name, VSAN, and members of the zoneset. In the following example we go through the steps to create the zoneset *ITSO_1* in *VSAN 11* and add the zone *Host_A_to_Disk*.

We right-click **Zonesets** and select **Insert** to create a new zone set as shown in Figure 4-75.


Edit Local Full Zone Database - /SAN/Fabric sc9509b
File
Edit
Tools
Zonesets
Zonesets
Zones
Host_
Aliase
DS_A
Host_
Insert...
Delete...
Convert Switch Port/FCID Members to pWWN...
Activate...
Deactivate...
Name
Read Only
QoS
QoS Priority
Broadcast
Members
Add to Zone or Alias
Activate...
Deactivate...
Distribute...
Close

VSAN: VSAN11
Switch: sc9216b

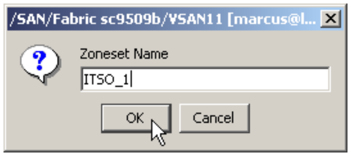
☐ Hide End Devices Currently Zoned by WWN

Type	Switch Interface	Name	WWN	FcId
	sc9216b fc1/2	DS_A	20:03:00:a0:b8:12:0f:13	0x290100
	sc9216b fc1/1	Qlogic 21:00:00:e0:8b:05:df:40	21:00:00:e0:8b:05:df:40	0x290000

Deleted 1 object.

Figure 4-75 Define new zone set

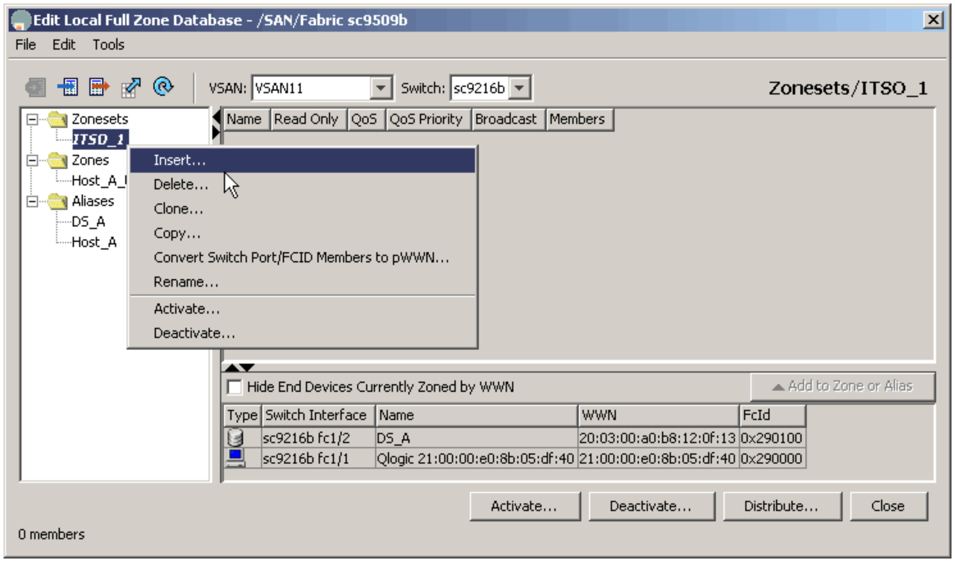
We define the name for the new zone set and click **OK**, as shown in Figure 4-76.


/SAN/Fabric sc9509b/VSAN11 [marcus@l...
OK
Cancel

Zoneset Name: ITSO_1

Figure 4-76 Name the Zone set

We right-click the created zone set *ITSO_1* and select **Insert** to define the members of the zone set, as shown in Figure 4-77.


Edit Local Full Zone Database - /SAN/Fabric sc9509b
File
Edit
Tools
Zonesets/ITSO_1
Zonesets
ITSO_1
Zones
Host_A_
Aliases
DS_A
Host_A
Name
Read Only
QoS
QoS Priority
Broadcast
Members
Insert...
Delete...
Clone...
Copy...
Convert Switch Port/FCID Members to pWWN...
Rename...
Activate...
Deactivate...
Hide End Devices Currently Zoned by WWN
Add to Zone or Alias
Activate...
Deactivate...
Distribute...
Close

VSAN: VSAN11
Switch: sc9216b

Type	Switch Interface	Name	WWN	FcId
	sc9216b fc1/2	DS_A	20:03:00:a0:b8:12:0f:13	0x290100
	sc9216b fc1/1	Qlogic 21:00:00:e0:8b:05:df:40	21:00:00:e0:8b:05:df:40	0x290000

0 members

Figure 4-77 Define zone members for the zone set

We select the Zone(s) to be member of the zone set and click **Add**, as shown in Figure 4-78.

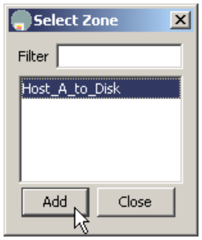
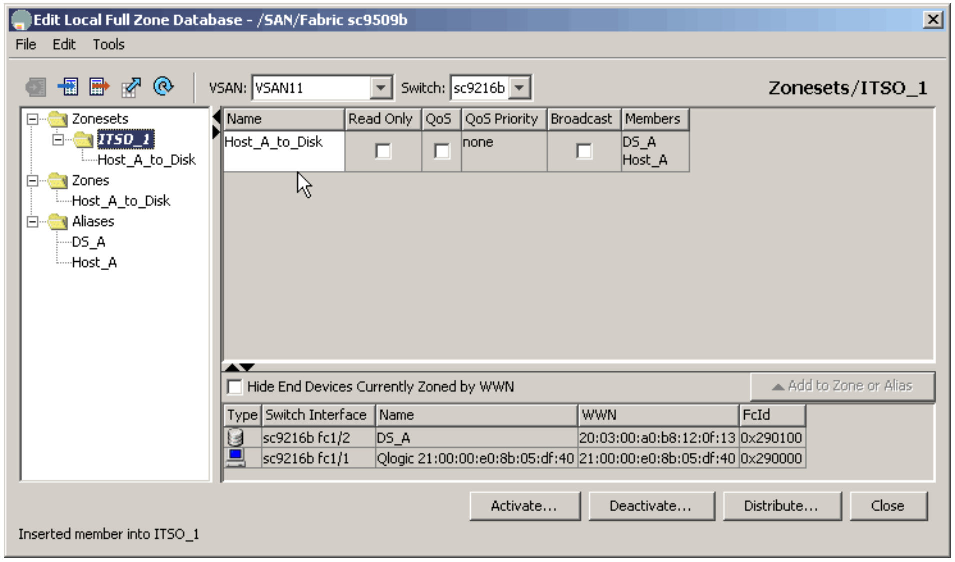

Select Zone
Filter
Host_A_to_Disk
Add
Close

Figure 4-78 Selecting the zone set member(s)

We verify that the zone set contains the member *Host_A_to_Disk* we have inserted, as shown in Figure 4-79.


Edit Local Full Zone Database - /SAN/Fabric sc9509b
File
Edit
Tools
Zonesets/ITSO_1
Zonesets
ITSO_1
Host_A_to_Disk
Zones
Host_A_to_Disk
Aliases
DS_A
Host_A
Hide End Devices Currently Zoned by WWN
Add to Zone or Alias
Activate...
Deactivate...
Distribute...
Close

VSAN: VSAN11 Switch: sc9216b

Name	Read Only	QoS	QoS Priority	Broadcast	Members
Host_A_to_Disk	☐	☐	none	☐	DS_A Host_A

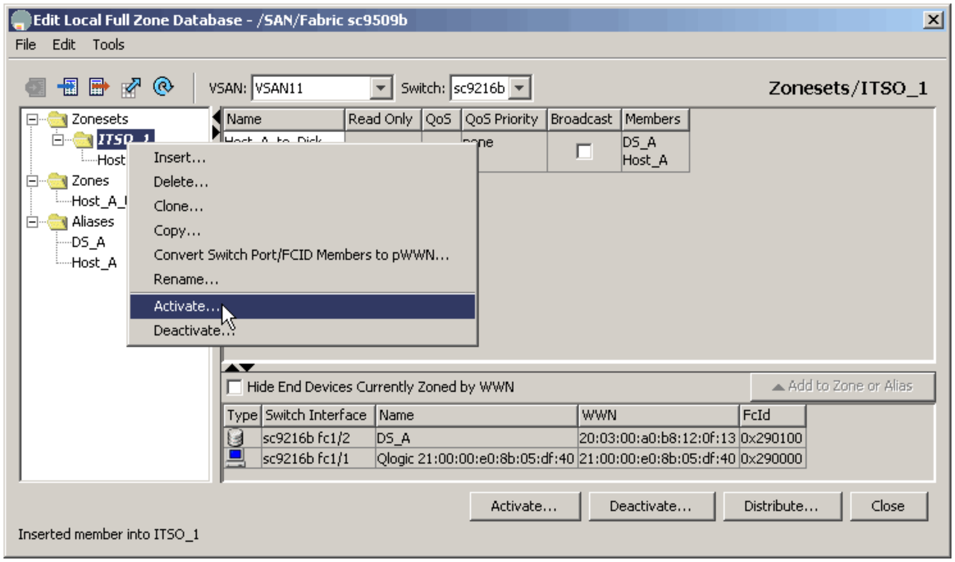
☐ Hide End Devices Currently Zoned by WWN

Type	Switch Interface	Name	WWN	FcId
	sc9216b fc1/2	DS_A	20:03:00:a0:b8:12:0f:13	0x290100
	sc9216b fc1/1	Qlogic 21:00:00:e0:8b:05:df:40	21:00:00:e0:8b:05:df:40	0x290000

Inserted member into ITSO_1

Figure 4-79 Listing the zone set

We right-click the zone set *ITSO_1* to activate the new zone set as shown in Figure 4-80.


Edit Local Full Zone Database - /SAN/Fabric sc9509b
File
Edit
Tools
Zonesets/ITSO_1
Zonesets
ITSO_1
Host
Zones
Host_A_
Aliases
DS_A
Host_A
Insert...
Delete...
Clone...
Copy...
Convert Switch Port/FCID Members to pWWN...
Rename...
Activate...
Deactivate...
Hide End Devices Currently Zoned by WWN
Add to Zone or Alias
Activate...
Deactivate...
Distribute...
Close

VSAN: VSAN11 Switch: sc9216b

Name	Read Only	QoS	QoS Priority	Broadcast	Members
Host_A_to_Disk			none	☐	DS_A Host_A

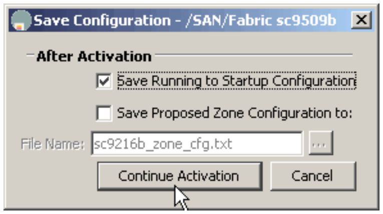
☐ Hide End Devices Currently Zoned by WWN

Type	Switch Interface	Name	WWN	FcId
	sc9216b fc1/2	DS_A	20:03:00:a0:b8:12:0f:13	0x290100
	sc9216b fc1/1	Qlogic 21:00:00:e0:8b:05:df:40	21:00:00:e0:8b:05:df:40	0x290000

Inserted member into ITSO_1

Figure 4-80 Activate the zone set

We are prompted if we want to save the running configuration to the startup configuration, and alternatively to a config file. We click **Continue Activation** to activate the configuration as shown in Figure 4-81.


Save Configuration - /SAN/Fabric sc9509b

After Activation

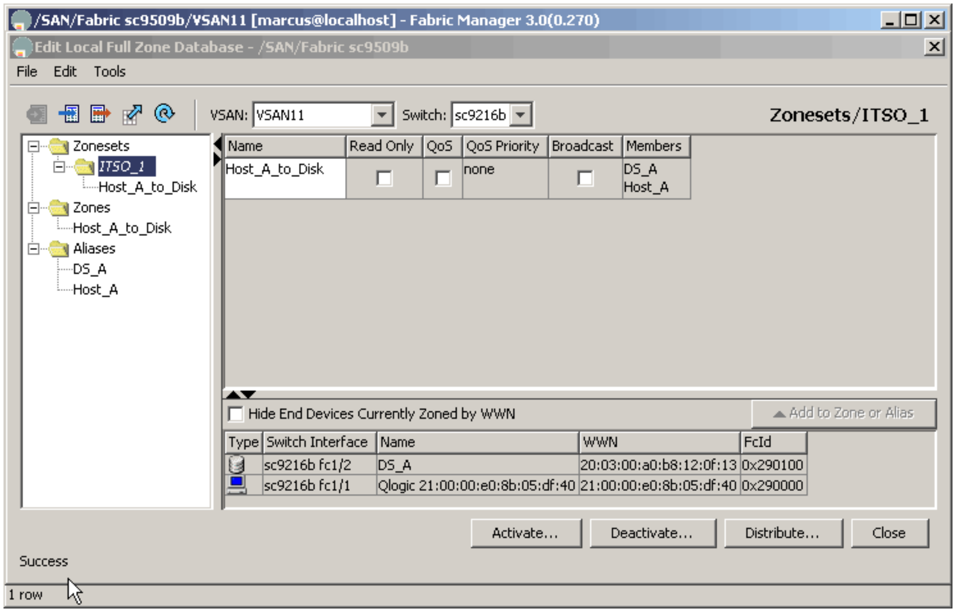
☑ Save Running to Startup Configuration

☐ Save Proposed Zone Configuration to:

File Name: sc9216b_zone_cfg.txt

Figure 4-81 Copying the zone set to the startup configuration

We monitor the status of the activation (and save to the startup configuration) at the bottom of the left corner as shown in Figure 4-82.


/SAN/Fabric sc9509b/VSAN11 [marcus@localhost] - Fabric Manager 3.0(0.270)

Edit Local Full Zone Database - /SAN/Fabric sc9509b

VSAN: VSAN11 Switch: sc9216b Zonesets/ITSO_1

- Zonesets
  - ITSO_1
    - Host_A_to_Disk
- Zones
  - Host_A_to_Disk
- Aliases
  - DS_A
  - Host_A

Name	Read Only	QoS	QoS Priority	Broadcast	Members
Host_A_to_Disk	☐	☐	none	☐	DS_A Host_A

☐ Hide End Devices Currently Zoned by WWN

Type	Switch Interface	Name	WWN	FcId
	sc9216b fc1/2	DS_A	20:03:00:a0:b8:12:0f:13	0x290100
	sc9216b fc1/1	Qlogic 21:00:00:e0:8b:05:df:40	21:00:00:e0:8b:05:df:40	0x290000

Success

1 row

Figure 4-82 Monitoring status for the zone set activation

Working with zone sets

When performing changes to the active zoneset, you actually work on a copy of the active zone set in the full zone set database. This means that any change does not take effect until you reactivate the zone set, since the active zoneset cannot be altered while active.

To illustrate this, we add the zone NewZone to the zone set *ITSO_1* and show that it does not apply to the activated zone set until we (re-)activate the zone set *ITSO_1*.

As shown in Example 4-22, we perform the following actions:

1. List zone sets for *VSAN11*.
2. List the active zone set.
3. Add the *NewZone* to *ITSO_1*.
4. List zone sets for VSAN11.
5. List the active zone set.
6. Reactivate the active zone set.
7. Verify that *NewZone* is part of the active zone set.

Example 4-22 Performing changes to the active zone set

```
1.
sc9216b# show zoneset vsan 11
zoneset name ITSO_1 vsan 11
  zone name Host_A_to_Disk vsan 11
    fcalias name DS_A vsan 11
      pwwn 20:03:00:a0:b8:12:0f:13

    fcalias name Host_A vsan 11
      fcid 0x290000

2.
sc9216b# show zoneset active vsan 11
zoneset name ITSO_1 vsan 11
  zone name Host_A_to_Disk vsan 11
  * fcid 0x290100 [pwwn 20:03:00:a0:b8:12:0f:13]
  * fcid 0x290000

3.
sc9216b(config)# zoneset name ITSO_1 vsan 11
sc9216b(config-zoneset)# member NewZone
sc9216b(config-zoneset)# end

4.
sc9216b# show zoneset vsan 11
zoneset name ITSO_1 vsan 11
  zone name Host_A_to_Disk vsan 11
```

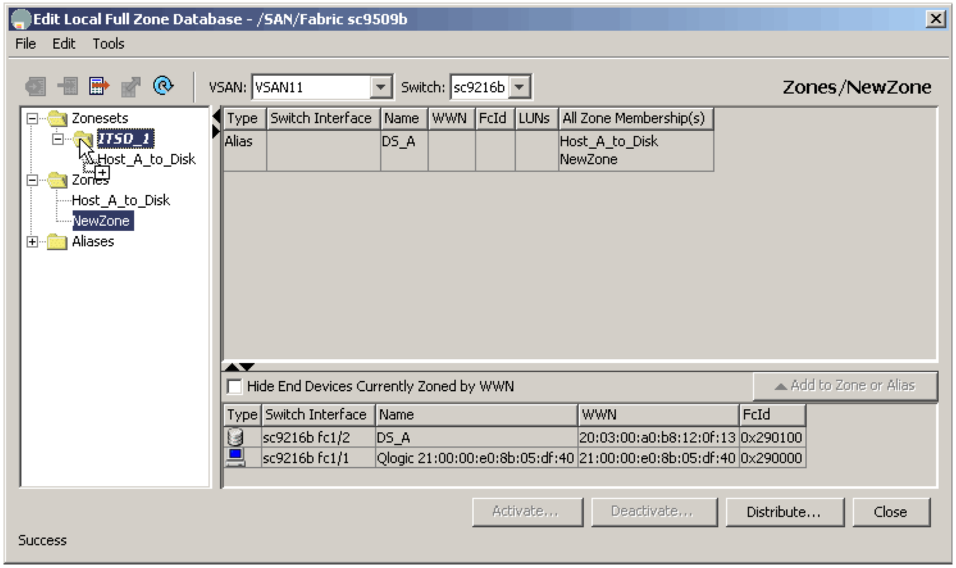
```
    fcalias name DS_A vsan 11
      pwwn 20:03:00:a0:b8:12:0f:13

    fcalias name Host_A vsan 11
      fcid 0x290000

  zone name NewZone vsan 11
    fcalias name DS_A vsan 11
      pwwn 20:03:00:a0:b8:12:0f:13

5.
sc9216b# show zoneset active vsan 11
zoneset name ITSO_1 vsan 11
  zone name Host_A_to_Disk vsan 11
  * fcid 0x290100 [pwwn 20:03:00:a0:b8:12:0f:13]
  * fcid 0x290000

6.
sc9216b(config)# zoneset activate name ITSO_1 vsan 11
Zoning database analysis vsan 11
Formatted database size: < 1 Kb ( < 1% usage)
 Active zoneset
  Ave. zone members: 2
  Formattted size: < 1 Kb
 Full zoning database
  Database not available
Zoneset activation initiated. check zone status

7.
sc9216b# show zoneset active
zoneset name ITSO_1 vsan 11
  zone name Host_A_to_Disk vsan 11
  * fcid 0x290100 [pwwn 20:03:00:a0:b8:12:0f:13]
  * fcid 0x290000

  zone name NewZone vsan 11
  * fcid 0x290100 [pwwn 20:03:00:a0:b8:12:0f:13]
```

When comparing step 5 with step 7 we notice that the *NewZone* has become part of the active zone set due to the activation of *ITSO_1* in step 6.

Working with zone sets using the GUI

When working with zone sets using the GUI, the same conditions apply, in that changes only take effect after you activate or reactivate the zone set.

In Figure 4-83 we drag the new zone onto the zone set.


Edit Local Full Zone Database - /SAN/Fabric sc9509b

VSAN: VSAN11 Switch: sc9216b

Zones/NewZone

Type	Switch Interface	Name	WWN	FcId	LUNs	All Zone Membership(s)
Alias		DS_A				Host_A_to_Disk NewZone

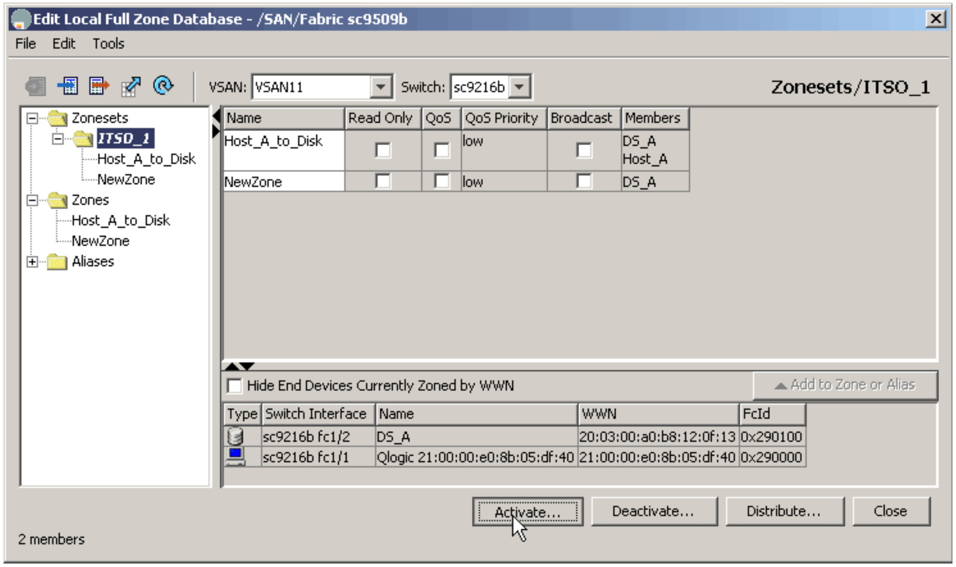
☐ Hide End Devices Currently Zoned by WWN

Type	Switch Interface	Name	WWN	FcId
	sc9216b fc1/2	DS_A	20:03:00:a0:b8:12:0f:13	0x290100
	sc9216b fc1/1	Qlogic 21:00:00:e0:8b:05:df:40	21:00:00:e0:8b:05:df:40	0x290000

Success
File
Edit
Tools
Zonesets
ITSO_1
Host_A_to_Disk
Zones
Host_A_to_Disk
NewZone
Aliases
Add to Zone or Alias
Activate...
Deactivate...
Distribute...
Close

Figure 4-83 Dragging the NewZone onto the zone set

In Figure 4-84 we reactivate the zone set.


Edit Local Full Zone Database - /SAN/Fabric sc9509b

VSAN: VSAN11 Switch: sc9216b

Zonesets/ITSO_1

Name	Read Only	QoS	QoS Priority	Broadcast	Members
Host_A_to_Disk	☐	☐	low	☐	DS_A Host_A
NewZone	☐	☐	low	☐	DS_A

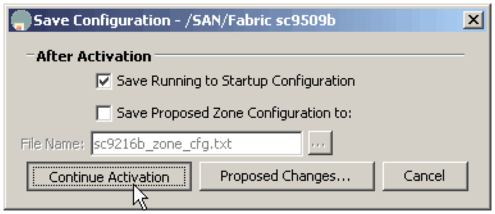
☐ Hide End Devices Currently Zoned by WWN

Type	Switch Interface	Name	WWN	FcId
	sc9216b fc1/2	DS_A	20:03:00:a0:b8:12:0f:13	0x290100
	sc9216b fc1/1	Qlogic 21:00:00:e0:8b:05:df:40	21:00:00:e0:8b:05:df:40	0x290000

2 members
File
Edit
Tools
Zonesets
ITSO_1
Host_A_to_Disk
NewZone
Zones
Host_A_to_Disk
NewZone
Aliases
Add to Zone or Alias
Activate...
Deactivate...
Distribute...
Close

Figure 4-84 Reactivating the zone set

In Figure 4-85 we save the change.


Save Configuration - /SAN/Fabric sc9509b
After Activation
Continue Activation
Proposed Changes...
Cancel

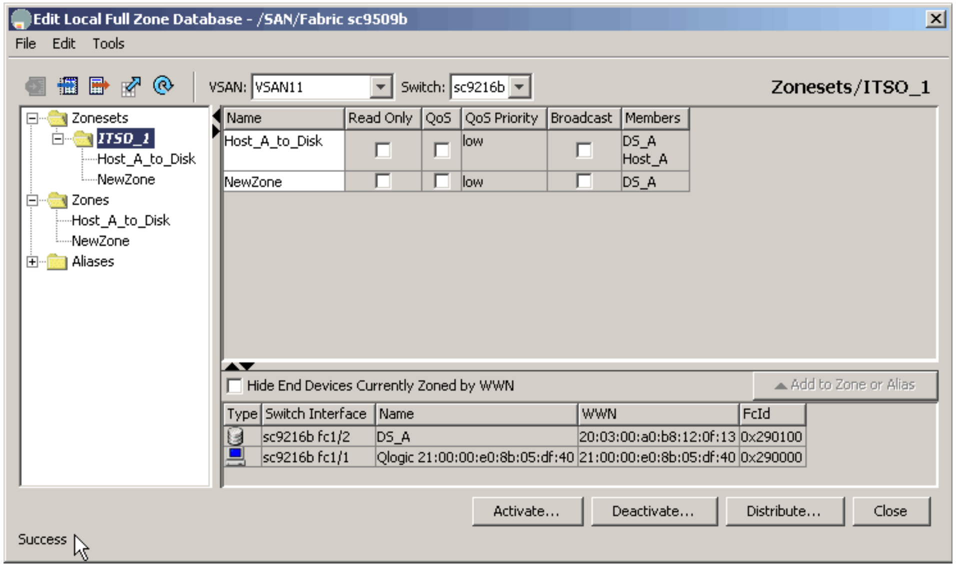
☑ Save Running to Startup Configuration

☐ Save Proposed Zone Configuration to:

File Name: sc9216b_zone_cfg.txt

Figure 4-85 Saving the change to the startup configuration

In Figure 4-86 we verify that the save is complete for our zone set.


Edit Local Full Zone Database - /SAN/Fabric sc9509b
File
Edit
Tools
Zonesets/ITSO_1
Zonesets
ITSO_1
Host_A_to_Disk
NewZone
Zones
Host_A_to_Disk
NewZone
Aliases
Add to Zone or Alias
Activate...
Deactivate...
Distribute...
Close

VSAN: VSAN11 Switch: sc9216b

Name	Read Only	QoS	QoS Priority	Broadcast	Members
Host_A_to_Disk	☐	☐	low	☐	DS_A Host_A
NewZone	☐	☐	low	☐	DS_A

☐ Hide End Devices Currently Zoned by WWN

Type	Switch Interface	Name	WWN	FcId
	sc9216b fc1/2	DS_A	20:03:00:a0:b8:12:0f:13	0x290100
	sc9216b fc1/1	Qlogic 21:00:00:e0:8b:05:df:40	21:00:00:e0:8b:05:df:40	0x290000

Success

Figure 4-86 Verifying the save to startup config is complete

Zone distribution

While all Cisco MDS 9000 family switches distribute the active zone sets when new E_Port links (ISL) appear, or when a new zone is activated in a VSAN, the full zone set is not distributed automatically.

To distribute the full zone set, this can be done either as *Config* or *EXEC mode*.

Config mode

The **`zoneset distribute VSAN`** command in config mode is used on a per VSAN basis to distribute the specified VSAN(s) to all switches along with the active zone set.

To configure distribution of the full zone set database of a VSAN along with the active zone set, we use the config command **`zoneset distribute full`**, as shown in Example 4-24.

Example 4-23

```
sc9216b# config t
Enter configuration commands, one per line.  End with CNTL/Z.
sc9216b(config)# zoneset distribute full vsan 11
```

EXEC mode

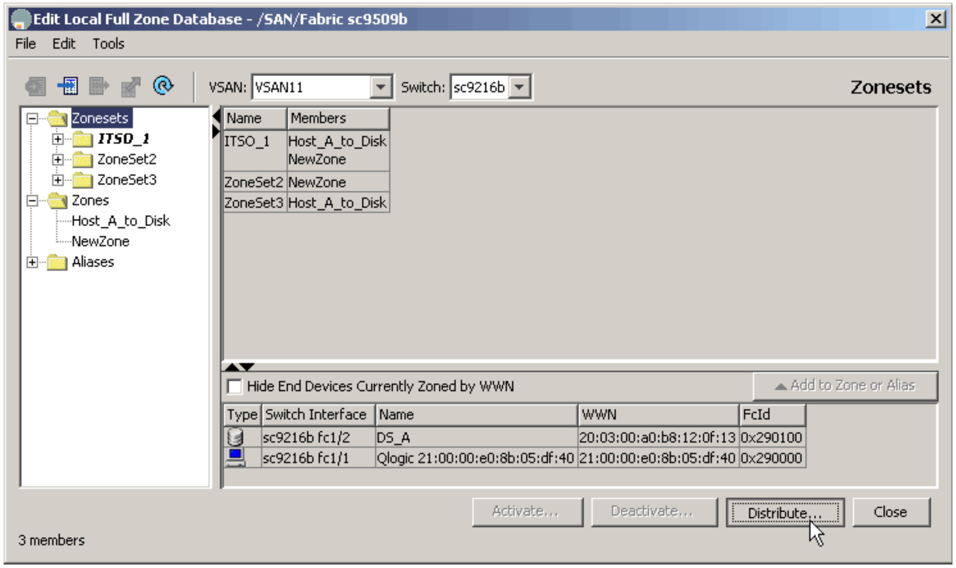
The **`zoneset distribute VSAN`** command in config mode is used to perform a one time distribution of all inactive, unmodified zone sets to all switches in the fabric.

To distribute the full zone set database of a VSAN, we use the command **`zoneset distribute`**. As shown in Example 4-24 we distribute the full zone set for VSAN 11, and then verify the zone set distribution completed using the command **`show zone status`**.

Example 4-24 Distributing the full zone set database for a VSAN

```
sc9216b# zoneset distribute vsan 11
Zoneset distribution initiated. check zone status

sc9216b# show zone status vsan 11
VSAN: 11 default-zone: deny distribute: active only Interop: default
    mode: basic merge-control: allow session: none
    hard-zoning: enabled
Default zone:
    qos: low broadcast: disabled ronly: disabled
Full Zoning Database :
    Zonesets:3  Zones:2 Aliases: 2
Active Zoning Database :
    Name: ITSO_1  Zonesets:1  Zones:2
Status: Zoneset distribution completed at 20:23:16 EST Nov 21 2005
```

To distribute the full zone set database using the GUI, we click **Distribute** as shown in Figure 4-87.


Edit Local Full Zone Database - /SAN/Fabric sc9509b
File
Edit
Tools
Zonesets
ITSO_1
ZoneSet2
ZoneSet3
Zones
Host_A_to_Disk
NewZone
Aliases
☐ Hide End Devices Currently Zoned by WWN
Add to Zone or Alias
Activate...
Deactivate...
Distribute...
Close
3 members

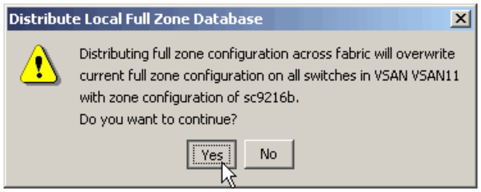
VSAN: VSAN11
Switch: sc9216b

Name	Members
ITSO_1	Host_A_to_Disk NewZone
ZoneSet2	NewZone
ZoneSet3	Host_A_to_Disk

Type	Switch Interface	Name	WWN	FcId
	sc9216b fc1/2	DS_A	20:03:00:a0:b8:12:0f:13	0x290100
	sc9216b fc1/1	Qlogic 21:00:00:e0:8b:05:df:40	21:00:00:e0:8b:05:df:40	0x290000

Figure 4-87 Distributing the full zone set database

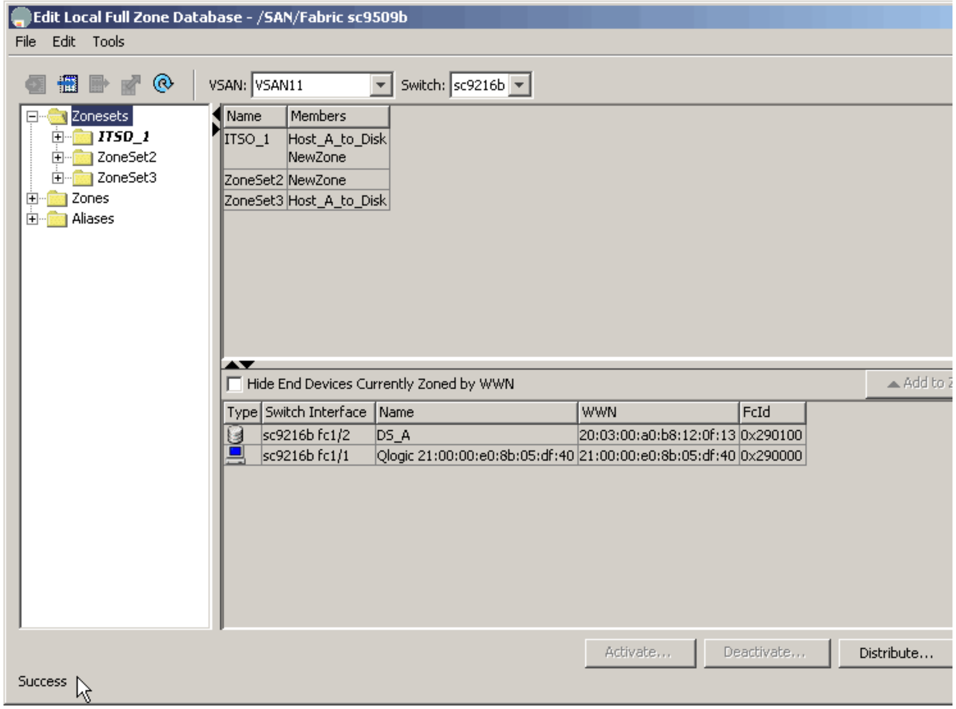
We are prompted to confirm zone set distribution since this will overwrite the current full zone configuration on all switches in VSAN 11, as shown in Figure 4-88.


Distribute Local Full Zone Database
Yes
No

Distributing full zone configuration across fabric will overwrite current full zone configuration on all switches in VSAN VSAN11 with zone configuration of sc9216b.
Do you want to continue?

Figure 4-88 Confirm distribution of full zone set database

Finally we verify completion of the zone set distribution as it is displayed in the lower left corner, shown in Figure 4-89.


Edit Local Full Zone Database - /SAN/Fabric sc9509b
File
Edit
Tools
Zonesets
ITSO_1
ZoneSet2
ZoneSet3
Zones
Aliases
Add to
Activate...
Deactivate...
Distribute...

VSAN: VSAN11
Switch: sc9216b

Name	Members
ITSO_1	Host_A_to_Disk NewZone
ZoneSet2	NewZone
ZoneSet3	Host_A_to_Disk

☐ Hide End Devices Currently Zoned by WWN

Type	Switch Interface	Name	WWN	FcId
	sc9216b fc1/2	DS_A	20:03:00:a0:b8:12:0f:13	0x290100
	sc9216b fc1/1	Qlogic 21:00:00:e0:8b:05:df:40	21:00:00:e0:8b:05:df:40	0x290000

Success

Figure 4-89 Verifying the status of the zone set distribution

> **Note:** When performing zone detracting, the full zone set database for the VSAN is only distributed across the fabric, and not saved to the startup configuration on the other switches (regardless of whether you use the CLI or GUI). Therefore you subsequently must perform this task on the other switches in the fabric.

4.6.12 LUN zoning

The LUN zoning feature, at the time of writing, is specific for the Cisco MDS family, and is not available in any interop mode. Since most storage devices used in today's production environments provide LUN masking, this feature is not extensively used, though it is available and can even be combined with LUN masking at the storage subsystem.

For details on how to configure LUN Masking, consult the MDS Cisco configuration Guide:

http://www.cisco.com/en/US/products/ps5989/products_installation_and_configuration_guides_list.html

4.6.13 Multiple switch environment

In the topics that follow, we show how to configure an inter switch link.

Inter switch link

An inter switch link (ISL) is created when connecting an E_Port (expansion port) of one switch to an E_Port on another switch. When we have multiple ISLs, these can be congregated to become a single “logical ISL” which, in Cisco terminology, is called a PortChannel.

Prior to establishing an ISL between two switches, we launch the *Merge Analysis* tool to verify that our existing VSANs can merge successfully across the fabric to avoid segmentation. In Figure 4-90 we click **Zone** and select **Merge Analysis** to launch the tool.

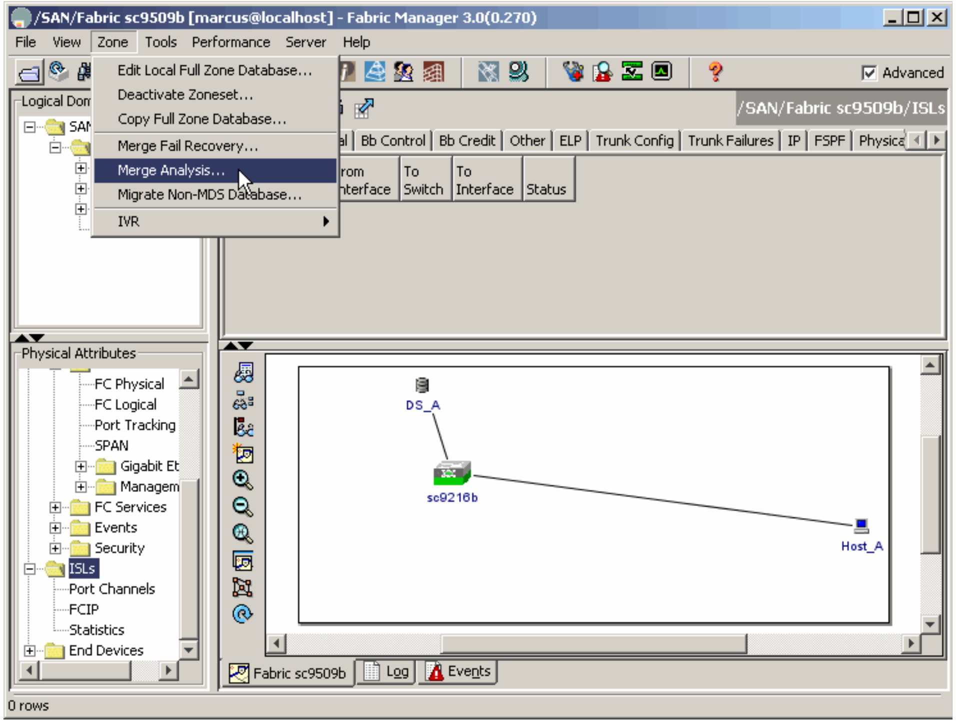
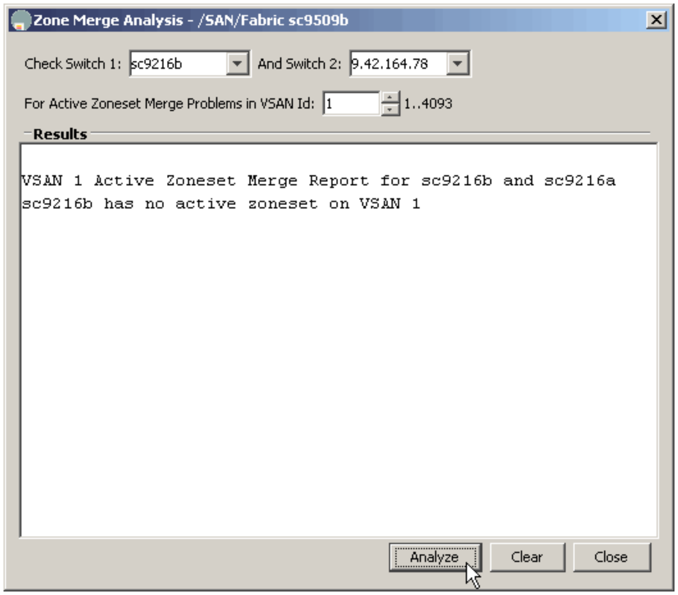

/SAN/Fabric sc9509b [marcus@localhost] - Fabric Manager 3.0(0.270)
File
View
Zone
Tools
Performance
Server
Help
Edit Local Full Zone Database...
Deactivate Zoneset...
Copy Full Zone Database...
Merge Fail Recovery...
Merge Analysis...
Migrate Non-MDS Database...
IVR
☑ Advanced
Logical Dom
SAN
/SAN/Fabric sc9509b/ISLs
al
Bb Control
Bb Credit
Other
ELP
Trunk Config
Trunk Failures
IP
FSPF
Physica
rom
nterface
To
Switch
To
Interface
Status
Physical Attributes
FC Physical
FC Logical
Port Tracking
SPAN
Gigabit Et
Managem
FC Services
Events
Security
ISLs
Port Channels
FCIP
Statistics
End Devices
DS_A
sc9216b
Host_A
Fabric sc9509b
Log
Events
0 rows

Figure 4-90 Launching the merge analysis tool

We then enter the IP address (or FQDN if all devices are defined in the DNS server), and click **Analyze**, shown in Figure 4-91, to analyze merge of VSAN1.


Zone Merge Analysis - /SAN/Fabric sc9509b
Results
Analyze
Clear
Close

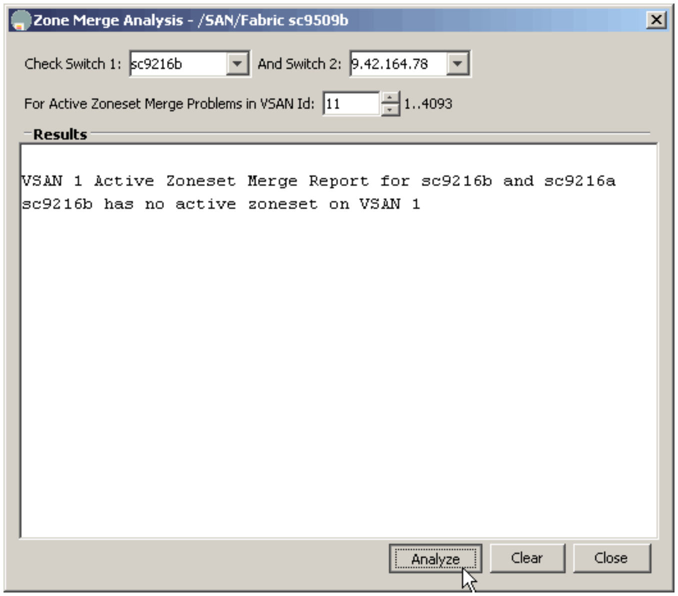
Check Switch 1: sc9216b And Switch 2: 9.42.164.78

For Active Zoneset Merge Problems in VSAN Id: 1 1..4093

```
VSAN 1 Active Zoneset Merge Report for sc9216b and sc9216a
sc9216b has no active zoneset on VSAN 1
```

Figure 4-91 Merge analysis for VSAN 1

To verify the merge of VSAN 11, we enter 11 in the VSAN Id box and click **Analyze**, as shown in Figure 4-92.


Zone Merge Analysis - /SAN/Fabric sc9509b
Analyze
Clear
Close

Check Switch 1: sc9216b And Switch 2: 9.42.164.78

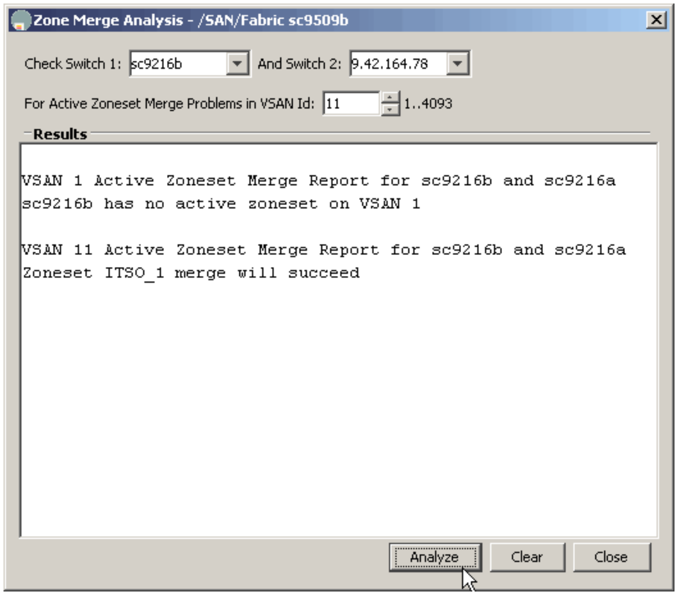
For Active Zoneset Merge Problems in VSAN Id: 11 1..4093

Results

```
VSAN 1 Active Zoneset Merge Report for sc9216b and sc9216a
sc9216b has no active zoneset on VSAN 1
```

Figure 4-92 Merge analysis for VSAN 11

We register the merge analysis results for VSAN 11, as shown in Figure 4-93.


Zone Merge Analysis - /SAN/Fabric sc9509b
Analyze
Clear
Close

Check Switch 1: sc9216b And Switch 2: 9.42.164.78

For Active Zoneset Merge Problems in VSAN Id: 11 1..4093

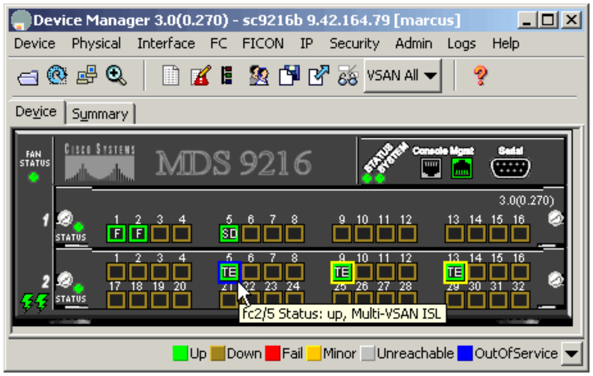
Results

```
VSAN 1 Active Zoneset Merge Report for sc9216b and sc9216a
sc9216b has no active zoneset on VSAN 1

VSAN 11 Active Zoneset Merge Report for sc9216b and sc9216a
Zoneset ITSO_1 merge will succeed
```

Figure 4-93 VSAN merge analysis verify merge to be successful

We are now ready to establish ISL(s) between the two switches.

We connect the two switches using three ISLs as shown in Figure 4-94, and depending on the trunk setting for the port, it becomes either an E_Port or a TE_Port. In our example, all ports are TE_Ports.


Device Manager 3.0(0.270) - sc9216b 9.42.164.79 [marcus]
Device Physical Interface FC FICON IP Security Admin Logs Help
VSAN All
Device Summary
FAN STATUS
Cisco Systems
MDS 9216
STATUS SYSTEM
Console Mgmt
Serial
3.0(0.270)
STATUS
F F SD
TE TE TE
🟩 Up 🟫 Down 🟥 Fail 🟨 Minor ⬜ Unreachable 🟦 OutOfService

fc2/5 Status: up, Multi-VSAN ISL

Figure 4-94 ISL connections, TE_Ports

After connecting the two switches, Fabric Manager shows the added switch and ISLs in the graphical presentation of the fabric, as shown in Figure 4-95.

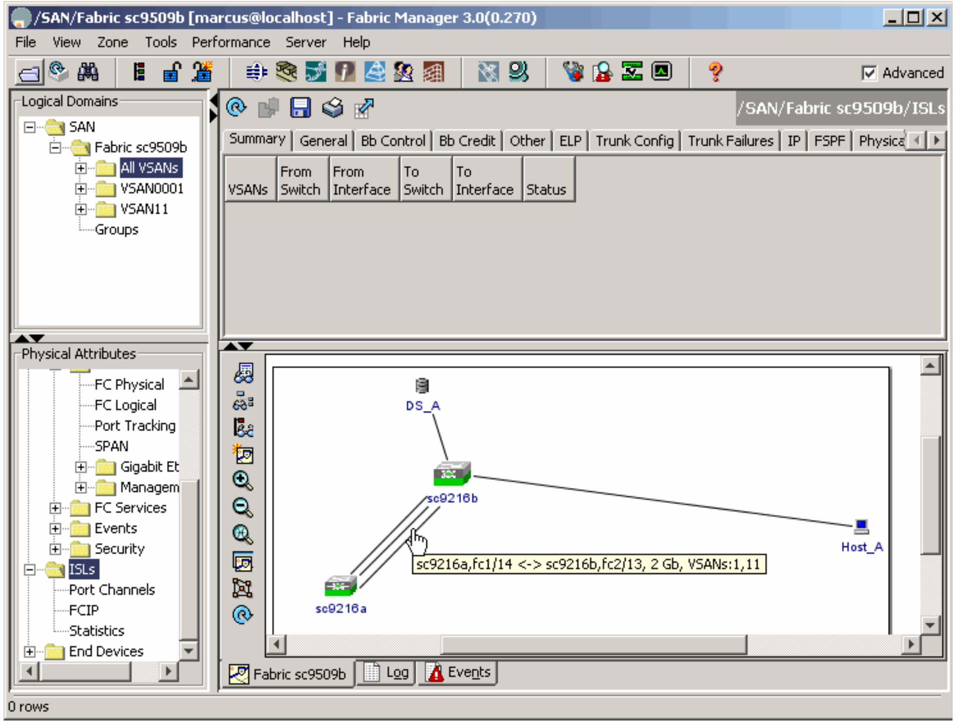

/SAN/Fabric sc9509b [marcus@localhost] - Fabric Manager 3.0(0.270)
File View Zone Tools Performance Server Help
Advanced
Logical Domains
SAN
Fabric sc9509b
All VSANs
VSAN0001
VSAN11
Groups
/SAN/Fabric sc9509b/ISLs
Summary General Bb Control Bb Credit Other ELP Trunk Config Trunk Failures IP FSPF Physica
VSANs
From Switch
From Interface
To Switch
To Interface
Status
Physical Attributes
FC Physical
FC Logical
Port Tracking
SPAN
Gigabit Et
Managem
FC Services
Events
Security
ISLs
Port Channels
FCIP
Statistics
End Devices
DS_A
sc9216b
Host_A
sc9216a
sc9216a,fc1/14 <-> sc9216b,fc2/13, 2 Gb, VSANs:1,11
Fabric sc9509b
Log
Events
0 rows

Figure 4-95 Fabric expanded by adding a switch

Trunking and PortChannel

In Cisco terminology, the term trunking is used to describe a single trunking E_Port (TE_Port) that can multiplex the traffic of more than one VSAN on a single physical interface. This is in contrast to other Fibre Channel switch manufacturers who use that term (trunking) to describe the aggregation of several physical interfaces into a single logical interface. Cisco calls this latter feature *PortChannel*.

Trunking and PortChannel features are available for both Fibre Channel and gigabit ethernet interfaces on the Cisco MDS 9000 family. Since the configuration rules for these features are different, we describe both of them separately.

FC trunking

Trunking, also known as VSAN trunking, enables interconnect ports to transmit and receive frames in more than one VSAN over the same physical link. In this case the link is configured as an extended ISL (EISL) link using the EISL frame format.

Trunking is only applicable to E_Ports and used for inter-switch connections. Trunking is normally enabled for all ports in the switch but can be disabled on a port-by-port basis. If the port becomes operational as a trunking E_Port, it is referred to as a TE_Port. If a port, with trunking enabled, is connected to a third-party switch, it works as a normal E_Port.

FC PortChannel

The PortChannel feature can be used to aggregate up to 16 ISL or EISL links into a single logical link. The Fibre Channel ports can be any Fibre Channel ports in any 16-port Fibre Channel line card.

The PortChannel feature increases the available aggregate bandwidth of the logical link since the traffic is distributed among all functional links in the channel. It also provides high availability, since the channel remains active as long as at least one of the links forming it remains active, and the traffic is transparently distributed over the remaining links.

Since PortChannel can be built on EISL links, both trunking and PortChannel are supported simultaneously.

Defining PortChannel using the CLI

In our setup we have the following EISLs:

Table 4-4 EISLs in our setup

sc9216a	sc9216b	Trunk
fc1/5	fc2/5	on
fc1/10	fc2/9	on
fc1/14	fc2/13	on

In Example 4-25 we define the PortChannel 1 to include all three EISLs between the switches sc9216a and sc9216b, which takes the EISL ports down. When we perform the **`no shutdown`** command, the ports come back up and the PortChannel is established; finally we list the PortChannel database on each switch, using the command **`show port-channel database`**.

Example 4-25 Setting up PortChannel

```
sc9216a# config t
Enter configuration commands, one per line.  End with CNTL/Z.
sc9216a(config-if)# interface fc1/5, fc1/10, fc1/14
sc9216a(config-if)# channel-group 1
fc1/5 fc1/10 fc1/14 added to port-channel 1 and disabled
please do the same operation on the switch at the other end of the
port-channel,
then do "no shutdown" at both ends to bring them up

sc9216b# config t
Enter configuration commands, one per line.  End with CNTL/Z.
sc9216b(config-if)# interface fc2/5, fc2/9, fc2/13
sc9216b(config-if)# channel-group 1
fc2/5 fc2/9 fc2/13 added to port-channel 1 and disabled
please do the same operation on the switch at the other end of the
port-channel,
then do "no shutdown" at both ends to bring them up

sc9216b(config-if)# no shutdown

sc9216a(config-if)# no shutdown

sc9216a# sho port-channel database
port-channel 1
    Administrative channel mode is on
    Operational channel mode is on
    Last membership update succeeded
    First operational port is fc1/5
    3 ports in total, 3 ports up
    Ports:   fc1/5    [up] *
             fc1/10   [up]
             fc1/14   [up]

port-channel 5
    Administrative channel mode is on
    Operational channel mode is on
    Last membership update succeeded
    No port

sc9216b# sho port-channel database
port-channel 1
    Administrative channel mode is on
    Operational channel mode is on
    Last membership update succeeded
    First operational port is fc2/5
    3 ports in total, 3 ports up
    Ports:   fc2/5    [up] *
             fc2/9    [up]
             fc2/13   [up]

port-channel 5
    Administrative channel mode is on
    Operational channel mode is on
    Last membership update succeeded
    No port
```

Note: When creating a PortChannel, a compatibility check is performed to ensure that all configuration parameters for each physical port in the channel are the same. Therefore a port cannot become operational if incompatibilities issues exist. For example, to enable trunk mode, all ports must be configured with trunk mode enabled prior to creating the PortChannel.

Tip: Using the force option when adding a port to a PortChannel forces the configuration of the ports in the PortChannel onto the added port to achieve compatibility.

4.6.14 Inter VSAN Routing (IVR)

VSANs provide the benefit to share the physical switch infrastructure while isolating traffic between VSANs. this inherently prevent resource sharing between VSANs. Using IVR provides resource sharing across VSANs without compromising the benefits of VSANs. IVR is done by specifying initiators and devices in different VSANs without merging the respective VSANs together.

Note: The Enterprise License Package (ENTERPRISE_PKG) must be installed on all IVR edge or transit switches.

To understand how IVR works, we first clarify the following IVR definitions:

- Inter VSAN Zone (IVZ): A set of end devices that are allowed to communicate across VSANs within their interconnected SAN fabric. This definition is based on their port World Wide Names (pWWNs) and their native VSAN associations. You can configure up to 200 IVZs and 2000 IVZ members on any switch in the Cisco MDS 9000 family.
- Inter VSAN Zone Sets (IVZS): One or more IVZs make up an IVZS. You can configure up to 32 IVZSs on any switch in the Cisco MDS 9000 family. Only one IVZS can be active at any time.

- Inter VSAN Path (IVR Path): An IVR path is a set of switches and inter-switch links through which a frame from one end-device in one VSAN can reach another end-device in some other VSAN. Multiple paths can exist between two such end-devices.
- Edge and Transit VSANs: A VSAN that initiates (source edge-VSAN) or terminates (destination edge-VSAN) an IVR path. Edge VSANs might be adjacent to each other or they might be connected by one or more transit VSANs

Here some guidelines to follow before IVR creation:

- Verify that unique domain IDs are configured in all switches and VSANs participating in IVR.

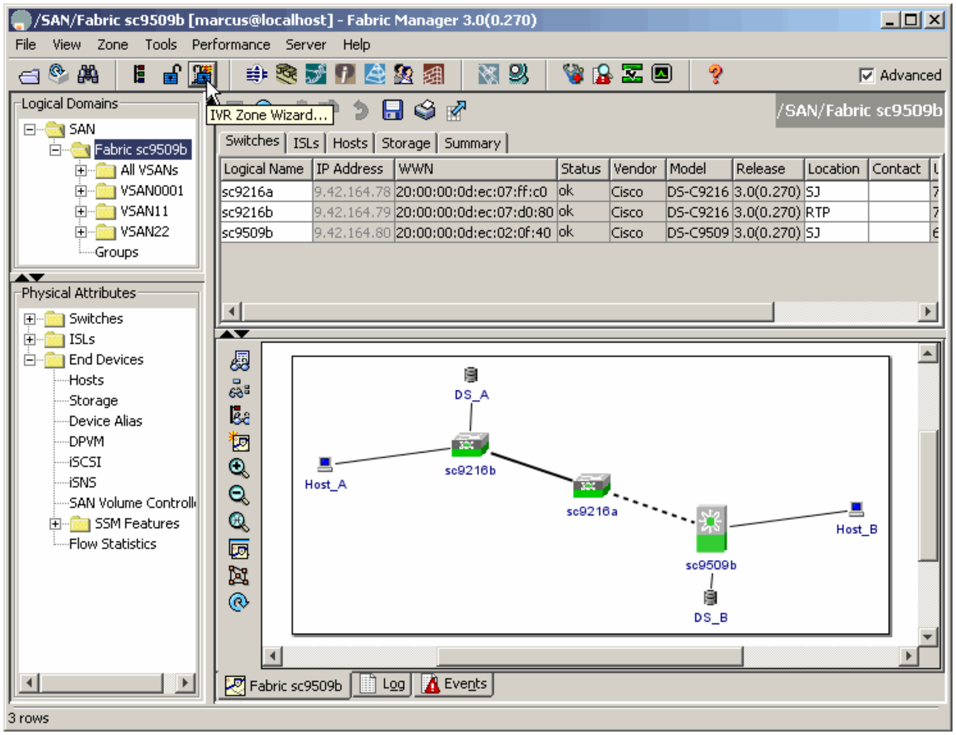
  > **Note:** Unique domain IDs are not a requirement when using IVR-NAT. A common domain ID (10, for example) could be in VSAN 5 and VSAN 6 and you could still route between devices in these VSANs attached to the switches with domain ID 10.

- Enable IVR in the border switches.
- Configure the required IVR topology in all the IVR-enabled border switches, or use the recommended auto-topology feature, which eliminates the necessity for the user to define one.
- Create and activate IVZSs in all the IVR-enabled border switches.
- Verify the IVR configuration.

Configuring IVR using the GUI

We now demonstrate a simple IVR to allow selected members of different VSANs to communicate.

The first step is to locate the *IVR Wizard*. It happens to be the same wizard that we use for normal zoning operations, and is found by starting with the Fabric Manager **IVR Wizard** icon, as seen in Figure 4-96.

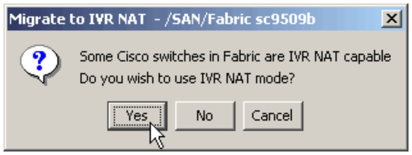


/SAN/Fabric sc9509b [marcus@localhost] - Fabric Manager 3.0(0.270)
File View Zone Tools Performance Server Help
☑ Advanced
IVR Zone Wizard...
/SAN/Fabric sc9509b
Logical Domains
SAN
Fabric sc9509b
All VSANs
VSAN0001
VSAN11
VSAN22
Groups
Physical Attributes
Switches
ISLs
End Devices
Hosts
Storage
Device Alias
DPVM
iSCSI
iSNS
SAN Volume Controll
SSM Features
Flow Statistics
Switches
ISLs
Hosts
Storage
Summary
DS_A
Host_A
sc9216b
sc9216a
sc9509b
Host_B
DS_B
Fabric sc9509b
Log
Events
3 rows

Logical Name	IP Address	WWN	Status	Vendor	Model	Release	Location	Contact
sc9216a	9.42.164.78	20:00:00:0d:ec:07:ff:c0	ok	Cisco	DS-C9216	3.0(0.270)	SJ	
sc9216b	9.42.164.79	20:00:00:0d:ec:07:d0:80	ok	Cisco	DS-C9216	3.0(0.270)	RTP	
sc9509b	9.42.164.80	20:00:00:0d:ec:02:0f:40	ok	Cisco	DS-C9509	3.0(0.270)	SJ	

Figure 4-96 Starting the IVR wizard

As we wish to use IVR NAT, we select the IVR NAT option, as shown in Figure 4-97.



Migrate to IVR NAT - /SAN/Fabric sc9509b
Yes
No
Cancel

Some Cisco switches in Fabric are IVR NAT capable
Do you wish to use IVR NAT mode?

Figure 4-97 Selecting IVR NAT

We continue with setting up our IVR by proceeding to the **Next** panel, where we have to move the VSANs we are working with to the appropriate window, as seen in Figure 4-98.

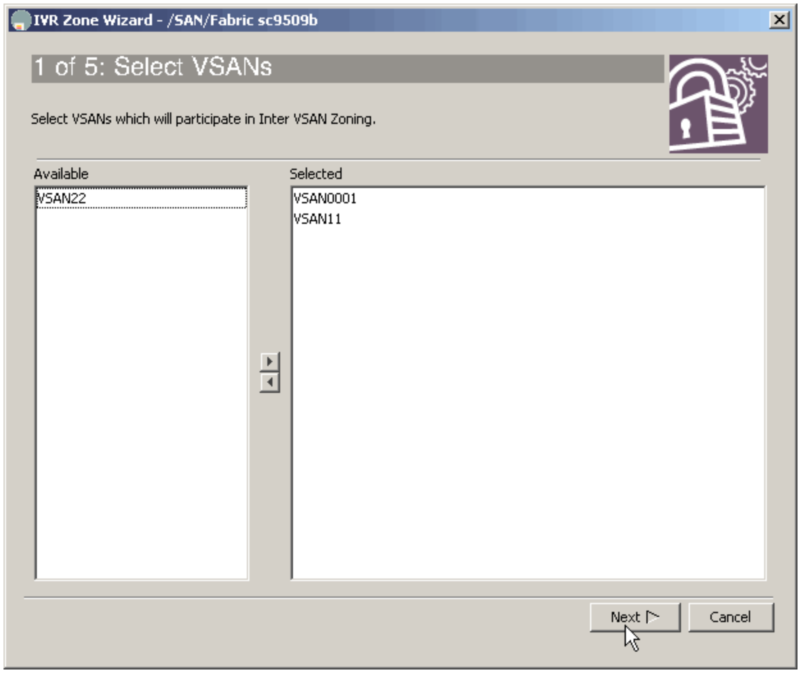
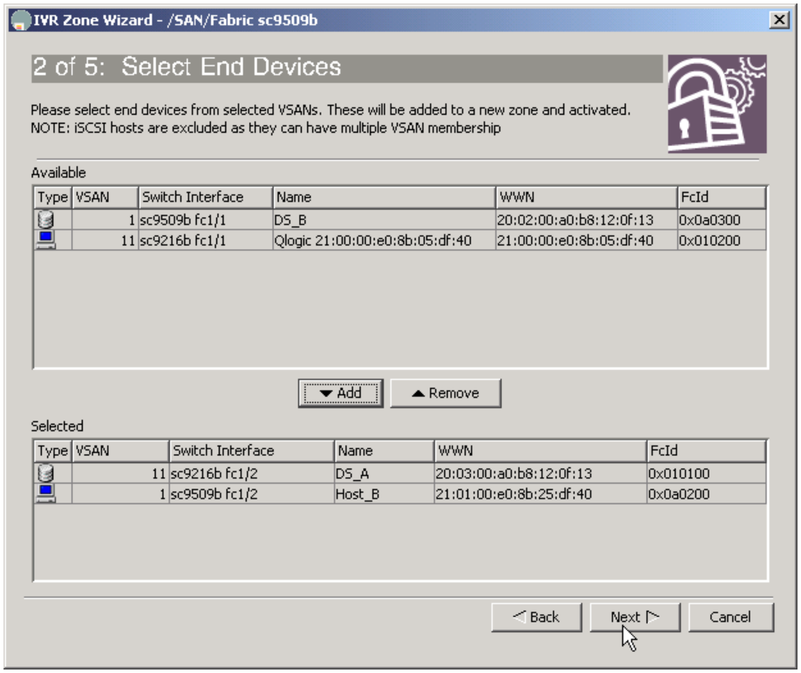

IVR Zone Wizard - /SAN/Fabric sc9509b
1 of 5: Select VSANs
Select VSANs which will participate in Inter VSAN Zoning.
Available
VSAN22
Selected
VSAN0001
VSAN11
Next
Cancel

Figure 4-98 Selecting VSANs

We proceed to the **Next** panel as shown in Figure 4-99.



2 of 5: Select End Devices

Please select end devices from selected VSANs. These will be added to a new zone and activated.
NOTE: iSCSI hosts are excluded as they can have multiple VSAN membership

Available

Type	VSAN	Switch Interface	Name	WWN	FcId
🗄	1	sc9509b fc1/1	DS_B	20:02:00:a0:b8:12:0f:13	0x0a0300
🖥	11	sc9216b fc1/1	Qlogic 21:00:00:e0:8b:05:df:40	21:00:00:e0:8b:05:df:40	0x010200

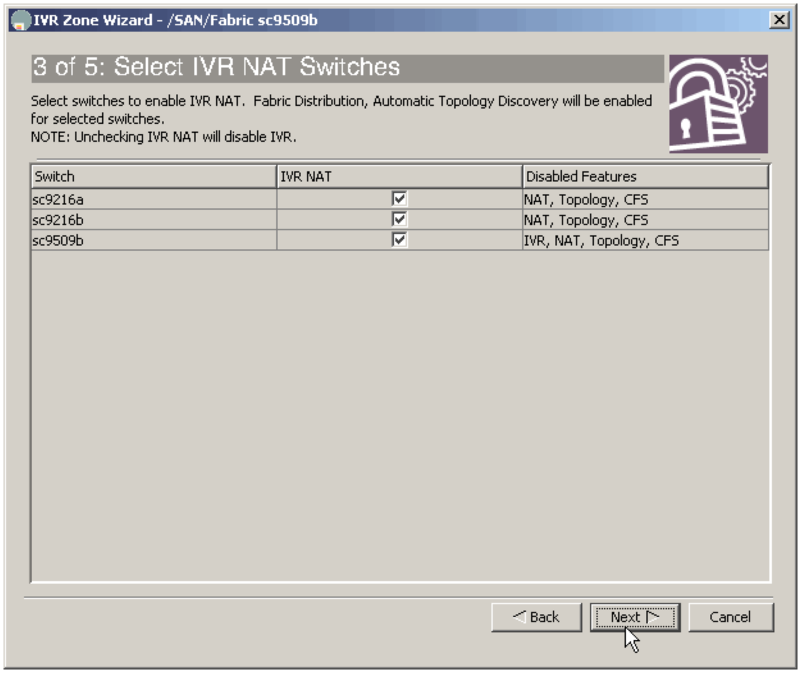
Selected

Type	VSAN	Switch Interface	Name	WWN	FcId
🗄	11	sc9216b fc1/2	DS_A	20:03:00:a0:b8:12:0f:13	0x010100
🖥	1	sc9509b fc1/2	Host_B	21:01:00:e0:8b:25:df:40	0x0a0200

Figure 4-99 Selecting end devices

After selecting the IVR NAT participants, we **Add** them to the **Selected** window, as seen in Figure 4-100.

> **Note:** Cisco MDS SAN-OS Release 2.1(1a) introduced IVR NAT, which allows you to set up IVR in a fabric without requiring unique domain IDs on every switch in the IVR path. When IVR NAT is enabled, the virtualized end device that appears in the native VSAN uses a virtual domain ID that is unique to the native VSAN.

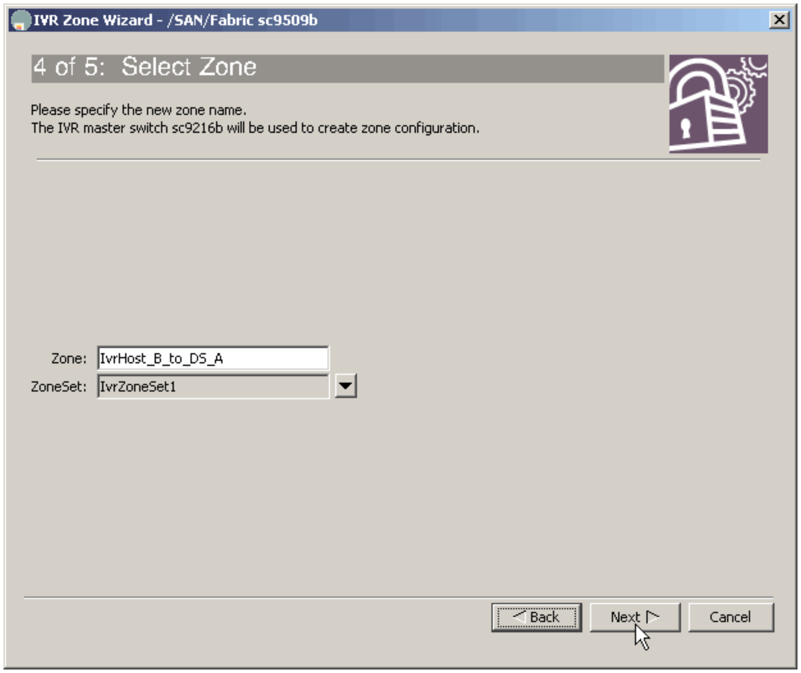

IVR Zone Wizard - /SAN/Fabric sc9509b
3 of 5: Select IVR NAT Switches
Back
Next
Cancel

Select switches to enable IVR NAT. Fabric Distribution, Automatic Topology Discovery will be enabled for selected switches.
NOTE: Unchecking IVR NAT will disable IVR.

Switch	IVR NAT	Disabled Features
sc9216a	☑	NAT, Topology, CFS
sc9216b	☑	NAT, Topology, CFS
sc9509b	☑	IVR, NAT, Topology, CFS

Figure 4-100 Selecting IVR switches

Now we have to specify the zone name as shown in Figure 4-101.


IVR Zone Wizard - /SAN/Fabric sc9509b

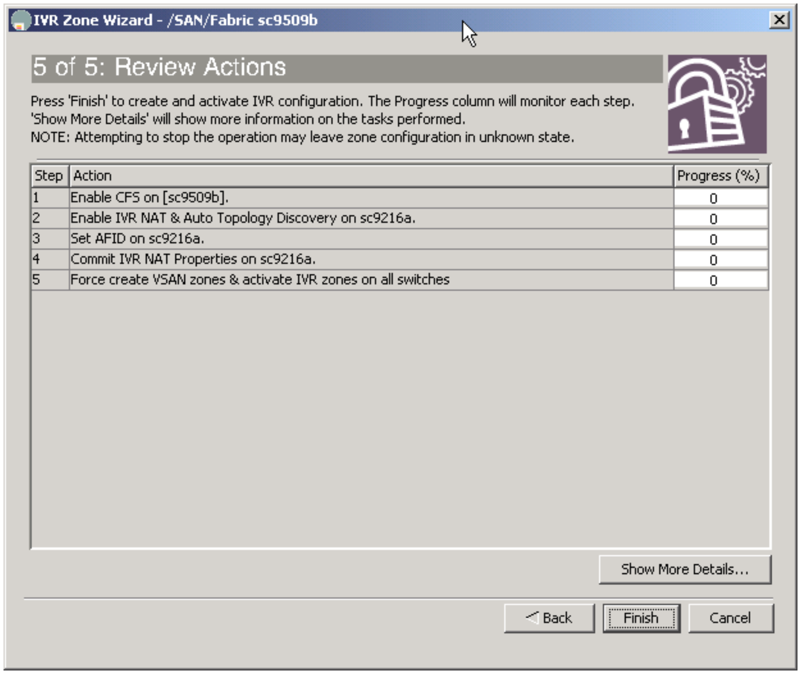
4 of 5: Select Zone

Please specify the new zone name.
The IVR master switch sc9216b will be used to create zone configuration.

Zone: IvrHost_B_to_DS_A
ZoneSet: IvrZoneSet1

Figure 4-101 Selecting the zone name

Now we can review our actions and the progress as seen in Figure 4-102.


IVR Zone Wizard - /SAN/Fabric sc9509b
Show More Details...
Back
Finish
Cancel

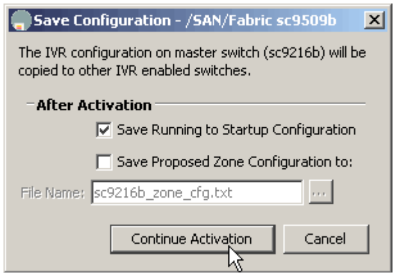
5 of 5: Review Actions

Press 'Finish' to create and activate IVR configuration. The Progress column will monitor each step.
'Show More Details' will show more information on the tasks performed.
NOTE: Attempting to stop the operation may leave zone configuration in unknown state.

Step	Action	Progress (%)
1	Enable CFS on [sc9509b].	0
2	Enable IVR NAT & Auto Topology Discovery on sc9216a.	0
3	Set AFID on sc9216a.	0
4	Commit IVR NAT Properties on sc9216a.	0
5	Force create VSAN zones & activate IVR zones on all switches	0

Figure 4-102 Review our actions

When we have done this, then we are asked if we want to continue with the activation to the startup configuration, or save it as a proposed configuration.


Save Configuration - /SAN/Fabric sc9509b
Continue Activation
Cancel

The IVR configuration on master switch (sc9216b) will be copied to other IVR enabled switches.

After Activation

☑ Save Running to Startup Configuration

☐ Save Proposed Zone Configuration to:

File Name: sc9216b_zone_cfg.txt

Figure 4-103 Confirm activation

We have now successfully configured our IVRs.

4.7 IP Services

When implementing any Cisco MDS 9000 family IP services module (as well as the MDS9216i), the traffic can be routed between any IP storage port and any other port on the Cisco MDS 9000 family switches in the fabric. It is configurable on a per port basis providing either Fibre Channel over IP (FCIP) or iSCSI on the defined port.

4.7.1 FCIP

To configure the IPS module for FCIP, you should have a basic understanding of the following concepts:

- FCIP and VE_Ports
- FCIP Links
- FCIP Profiles
- FCIP Interfaces

FCIP and VE_Ports describes the internal model of FCIP with respect to Fibre Channel inter switch links (ISLs) and Cisco's enhanced ISLs (EISLs).

FCIP defines virtual E (VE) ports, which behave exactly like standard Fibre Channel E_Ports, except that the transport in this case is FCIP instead of Fibre Channel. The only requirement is for the other end of the VE_Port to be another VE_Port. A virtual ISL is established over an FCIP link and transports Fibre Channel traffic. Each associated virtual ISL looks like a Fibre Channel ISL with either an E_Port or a TE_Port at each end.

FCIP links consist of one or more TCP connections between two FCIP link end points. Each link carries encapsulated Fibre Channel frames. When the FCIP link comes up, the VE_Ports at both ends of the FCIP link create a virtual Fibre Channel (E)ISL and initiate the E_Port protocol to bring up the (E)ISL. By default, the FCIP feature on any Cisco MDS 9000 family switch creates two TCP connections for each FCIP link.

- One connection is used for data frames.
- The second connection is used only for Fibre Channel control frames, that is, switch-to-switch protocol frames (all Class F) frames. This arrangement is used to provide low latency for all control frames.

To enable FCIP on the IPS module, an FCIP profile and FCIP interface (interface FCIP) must be configured. The FCIP link is established between two peers, the VE_Port initialization behavior is identical to a normal E_Port. This behavior is independent of the link being FCIP or pure Fibre Channel, and is based on the E_Port discovery process (ELP, ESC). When the FCIP link is established, the VE_Port behavior is identical to E_Port behavior for all inter-switch communication (including domain management, zones, and VSANs). At the Fibre Channel layer, all VE and E_Port operations are identical.

The FCIP profile contains information about local IP address and TCP parameters. The profile defines the following information:

- The local connection points (IP address and TCP port number)
- The behavior of the underlying TCP connections for all FCIP links that use this profile

The FCIP profiles local IP address determines the Gigabit Ethernet port where the FCIP links terminates.

The FCIP interface is the local endpoint of the FCIP link and a VE_Port interface. All the FCIP and E_Port parameters are configured in context to the FCIP interface.

The FCIP profile determines which Gigabit Ethernet port initiates the FCIP links and defines the TCP connection behavior.

The FCIP parameters consist of the following data:

- Peer information.
- Number of TCP connections for the FCIP link.
- E_Port parameters--trunking mode and trunk allowed VSAN list.

Setting up FCIP

Setting up FCIP is a step by step process, and in the following sections we perform each of the following steps to set up FCIP using the CLI:

1. Enable FCIP
2. Configure the GigE interface.
3. Create an FCIP profile and assign the GigE interface IP address.
4. Create an FCIP interface and assign the FCIP profile.
5. Configure the peer IP address for the FCIP interface.
6. Enable the FCIP interface.

Enable FCIP

To enable FCIP, we use the command **`fcip enable`** as shown in Example 4-26, and we are notified that we are using a temporary license (this must be done on both switches).

Note: Prior to setting up FCIP, we must enable the FCIP feature on the switches, since it is disabled per default on all switches.

When enabling FCIP, it is verified if you have a current SAN_EXTN_OVER_IP license.

Example 4-26 Enabling FCIP

```
sc9216a# config t
Enter configuration commands, one per line.  End with CNTL/Z.
sc9216a(config)# fcip enable
SAN_EXTN_OVER_IP license not installed. IP Storage feature will be shutdown
after grace period of approximately 92 day(s).
Ssc9216a(config)#
```

Configure GigE interface

In Example 4-27, we assign an IP address (10.1.1.21/24) on switch *sc9216a* to the GigE interface *GigabitEthernet2/1*, and on the switch *sc9509b*, we assign an IP address (10.1.1.41/24) to the interface *GigabitEthernet4/1.*

Example 4-27 Configure the GigE interface

```
sc9216a# config t
Enter configuration commands, one per line.  End with CNTL/Z.
sc9216a(config)# interface GigabitEthernet2/1
sc9216a(config-if)# ip address 10.1.1.21 255.255.255.0

sc9509b# config t
Enter configuration commands, one per line.  End with CNTL/Z.
sc9509b(config)# interface GigabitEthernet4/1
sc9509b(config-if)# ip address 10.1.1.41 255.255.255.0
```

Create FCIP Profile

Next we create the FCIP profile, as shown in Example 4-28.

Example 4-28 Create FCIP profile

```
sc9216a# config t
Enter configuration commands, one per line.  End with CNTL/Z.
sc9216a(config)# fcip profile 99
sc9216a(config-profile)# ip address 10.1.1.21

sc9509b# config t
Enter configuration commands, one per line.  End with CNTL/Z.
sc9509b(config)# fcip profile 99
sc9509b(config-profile)# ip address 10.1.1.41
```

Create FCIP Interface

In Example 4-29 we create the FCIP interface.

Example 4-29 Create FCIP interface

```
sc9216a# config t
Enter configuration commands, one per line.  End with CNTL/Z.
sc9216a(config)# interface fcip 99
sc9216a(config-if)# use-profile 99
sc9216a(config-if)# peer info address 10.1.1.41
sc9216a(config-if)# no shutdown

sc9509b# config t
Enter configuration commands, one per line.  End with CNTL/Z.
sc9509b(config)# interface fcip 99
sc9509b(config-if)# use-profile 99
sc9509b(config-if)# peer-info ipaddr 10.1.1.21
sc9509b(config-if)# no shutdown
```

In Example 4-30 we show the FCIP interfaces and profiles.

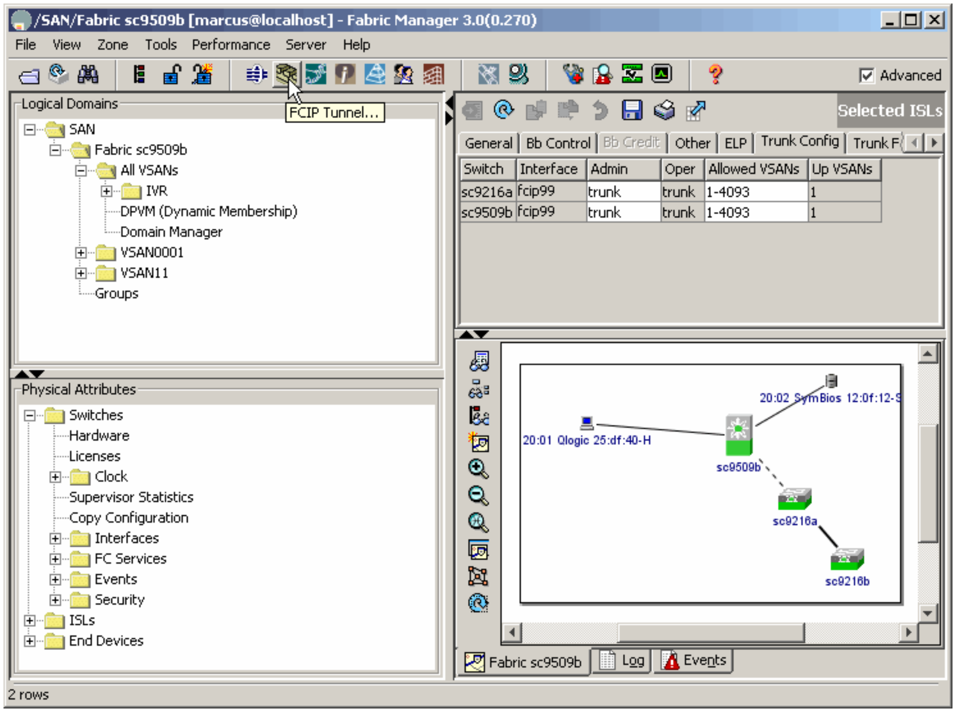
Example 4-30 Using the show fcip summary command

```
sc9216a# show fcip summary
-------------------------------------------------------------------------------
Tun prof    Eth-if    peer-ip       Status T W T Enc Comp  Bandwidth   rtt
                                           E A A            max/min    (us)
-------------------------------------------------------------------------------
99   99  GE2/1      10.1.1.41        TRNK  Y N N  N   N    1000M/500M  1000

sc9509b# show fcip summary
-------------------------------------------------------------------------------
Tun prof    Eth-if    peer-ip       Status T W T Enc Comp  Bandwidth   rtt
                                           E A A            max/min    (us)
-------------------------------------------------------------------------------
99   99  GE4/1      10.1.1.21        TRNK  Y N N  N   N    1000M/500M  1000
```

We have now set up FCIP.

4.7.2 Creating an FCIP tunnel using the GUI

Now we show how to use the GUI to create the FCIP tunnel. In Figure 4-104 we show how to locate the FCIP wizard.

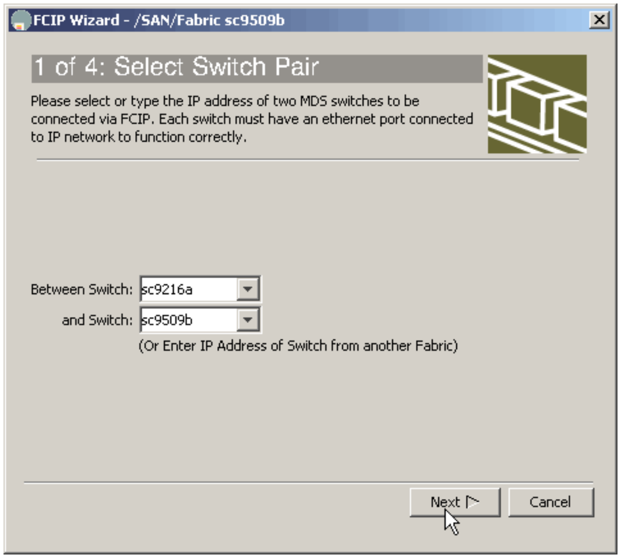


/SAN/Fabric sc9509b [marcus@localhost] - Fabric Manager 3.0(0.270)
File View Zone Tools Performance Server Help
☑ Advanced
FCIP Tunnel...
Logical Domains
SAN
Fabric sc9509b
All VSANs
IVR
DPVM (Dynamic Membership)
Domain Manager
VSAN0001
VSAN11
Groups
Physical Attributes
Switches
Hardware
Licenses
Clock
Supervisor Statistics
Copy Configuration
Interfaces
FC Services
Events
Security
ISLs
End Devices
Selected ISLs
General
Bb Control
Bb Credit
Other
ELP
Trunk Config
Trunk F
20:02 SymBios 12:0f:12-S
20:01 Qlogic 25:df:40-H
sc9509b
sc9216a
sc9216b
Fabric sc9509b
Log
Events
2 rows

Switch	Interface	Admin	Oper	Allowed VSANs	Up VSANs
sc9216a	fcip99	trunk	trunk	1-4093	1
sc9509b	fcip99	trunk	trunk	1-4093	1

Figure 4-104 Starting the FCIP wizard

When the wizard starts, we select the switch pair to establish the link between as shown in Figure 4-105.



1 of 4: Select Switch Pair

Please select or type the IP address of two MDS switches to be connected via FCIP. Each switch must have an ethernet port connected to IP network to function correctly.

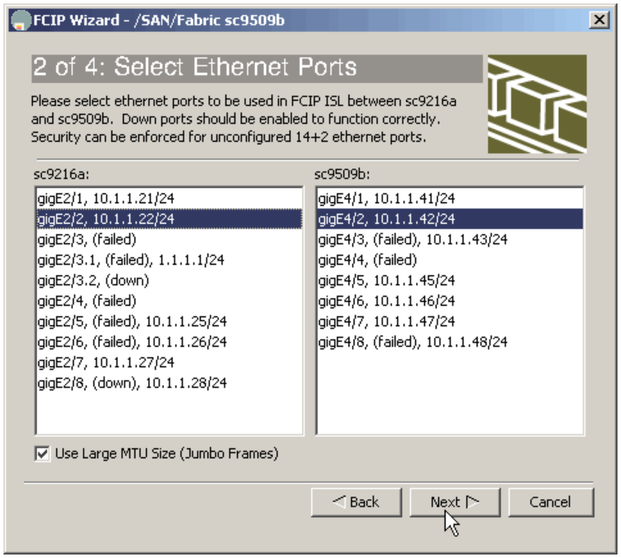
Between Switch: sc9216a

and Switch: sc9509b

(Or Enter IP Address of Switch from another Fabric)

Figure 4-105 Selecting switch pair

We then select the Ethernet ports to use, as shown in Figure 4-106.



2 of 4: Select Ethernet Ports

Please select ethernet ports to be used in FCIP ISL between sc9216a and sc9509b. Down ports should be enabled to function correctly. Security can be enforced for unconfigured 14+2 ethernet ports.

sc9216a:

- gigE2/1, 10.1.1.21/24
- gigE2/2, 10.1.1.22/24
- gigE2/3, (failed)
- gigE2/3.1, (failed), 1.1.1.1/24
- gigE2/3.2, (down)
- gigE2/4, (failed)
- gigE2/5, (failed), 10.1.1.25/24
- gigE2/6, (failed), 10.1.1.26/24
- gigE2/7, 10.1.1.27/24
- gigE2/8, (down), 10.1.1.28/24

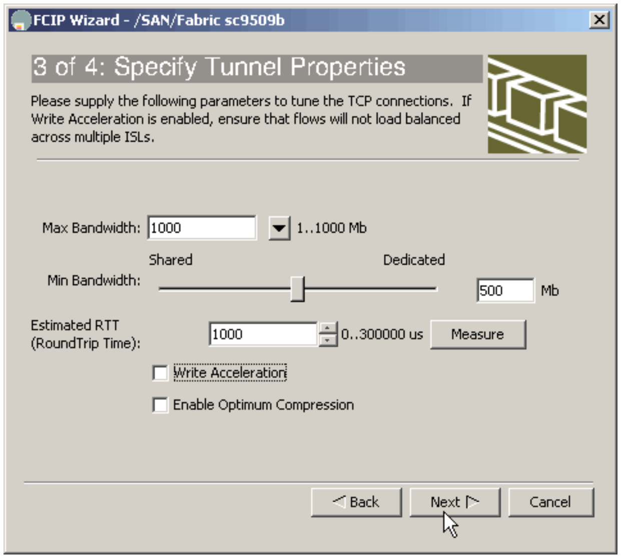
sc9509b:

- gigE4/1, 10.1.1.41/24
- gigE4/2, 10.1.1.42/24
- gigE4/3, (failed), 10.1.1.43/24
- gigE4/4, (failed)
- gigE4/5, 10.1.1.45/24
- gigE4/6, 10.1.1.46/24
- gigE4/7, 10.1.1.47/24
- gigE4/8, (failed), 10.1.1.48/24

☑ Use Large MTU Size (Jumbo Frames)

Figure 4-106 Selecting the Ethernet ports

We then specify the tunnel properties, as shown in Figure 4-107.



FCIP Wizard - /SAN/Fabric sc9509b

3 of 4: Specify Tunnel Properties

Please supply the following parameters to tune the TCP connections. If Write Acceleration is enabled, ensure that flows will not load balanced across multiple ISLs.

Max Bandwidth: 1000 1..1000 Mb

Min Bandwidth: Shared — Dedicated 500 Mb

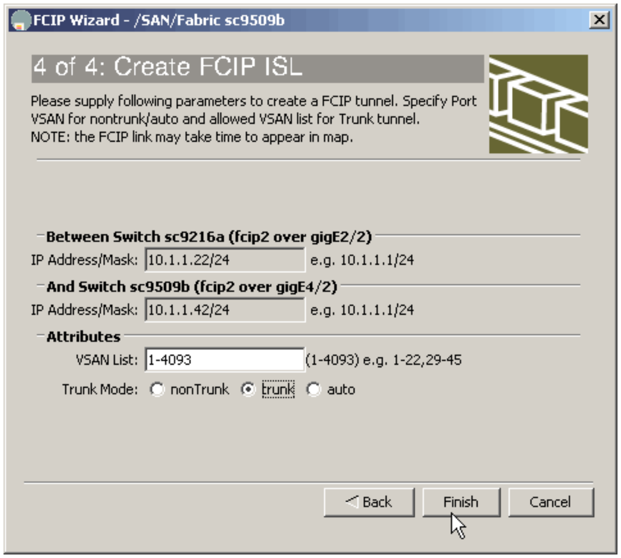
Estimated RTT (RoundTrip Time): 1000 0..300000 us

☐ Write Acceleration

☐ Enable Optimum Compression

Figure 4-107 Specifying TCP properties for the tunnel

In Figure 4-108 we show how to create the FCIP ISL with the properties we want.



FCIP Wizard - /SAN/Fabric sc9509b

4 of 4: Create FCIP ISL

Please supply following parameters to create a FCIP tunnel. Specify Port VSAN for nontrunk/auto and allowed VSAN list for Trunk tunnel.
NOTE: the FCIP link may take time to appear in map.

Between Switch sc9216a (fcip2 over gigE2/2)

IP Address/Mask: 10.1.1.22/24 e.g. 10.1.1.1/24

And Switch sc9509b (fcip2 over gigE4/2)

IP Address/Mask: 10.1.1.42/24 e.g. 10.1.1.1/24

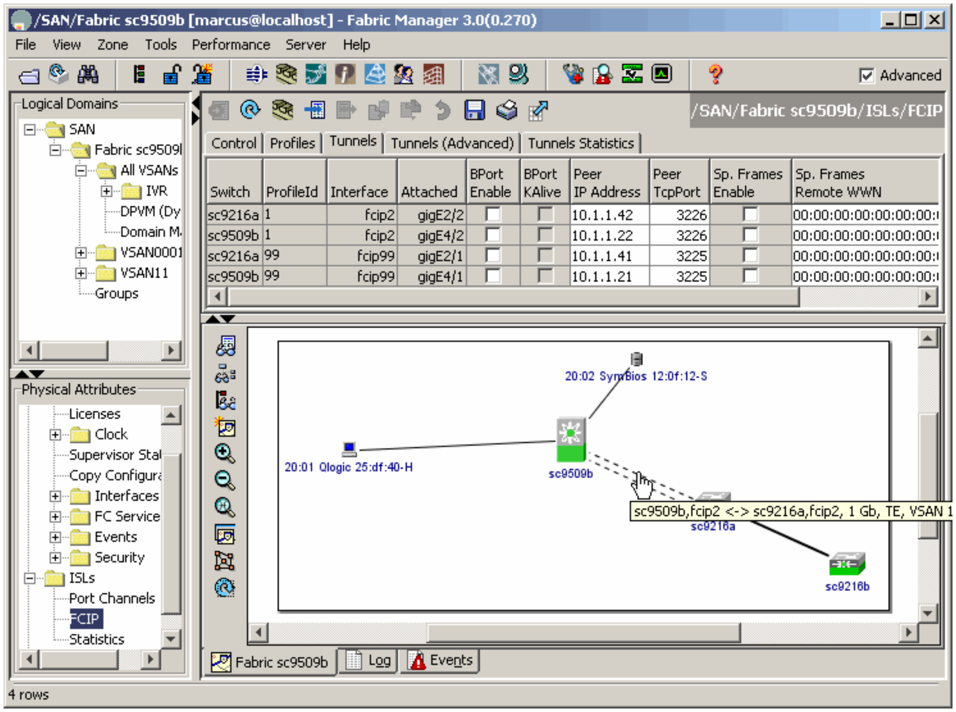
Attributes

VSAN List: 1-4093 (1-4093) e.g. 1-22,29-45

Trunk Mode: ○ nonTrunk ● trunk ○ auto

Figure 4-108 Specifying ISL properties for the FCIP tunnel

In Figure 4-109 we show the tunnel we have created.


/SAN/Fabric sc9509b [marcus@localhost] - Fabric Manager 3.0(0.270)
File View Zone Tools Performance Server Help
☑ Advanced
/SAN/Fabric sc9509b/ISLs/FCIP
Logical Domains
SAN
Fabric sc9509l
All VSANs
IVR
DPVM (Dy
Domain M
VSAN0001
VSAN11
Groups
Physical Attributes
Licenses
Clock
Supervisor Stat
Copy Configur
Interfaces
FC Service
Events
Security
ISLs
Port Channels
FCIP
Statistics
Control
Profiles
Tunnels
Tunnels (Advanced)
Tunnels Statistics
20:02 Symbios 12:0f:12-S
20:01 Qlogic 25:df:40-H
sc9509b
sc9216a
sc9216b
Fabric sc9509b
Log
Events

Switch	ProfileId	Interface	Attached	BPort Enable	BPort KAlive	Peer IP Address	Peer TcpPort	Sp. Frames Enable	Sp. Frames Remote WWN
sc9216a	1	fcip2	gigE2/2	☐	☐	10.1.1.42	3226	☐	00:00:00:00:00:00:00:
sc9509b	1	fcip2	gigE4/2	☐	☐	10.1.1.22	3226	☐	00:00:00:00:00:00:00:
sc9216a	99	fcip99	gigE2/1	☐	☐	10.1.1.41	3225	☐	00:00:00:00:00:00:00:
sc9509b	99	fcip99	gigE4/1	☐	☐	10.1.1.21	3225	☐	00:00:00:00:00:00:00:

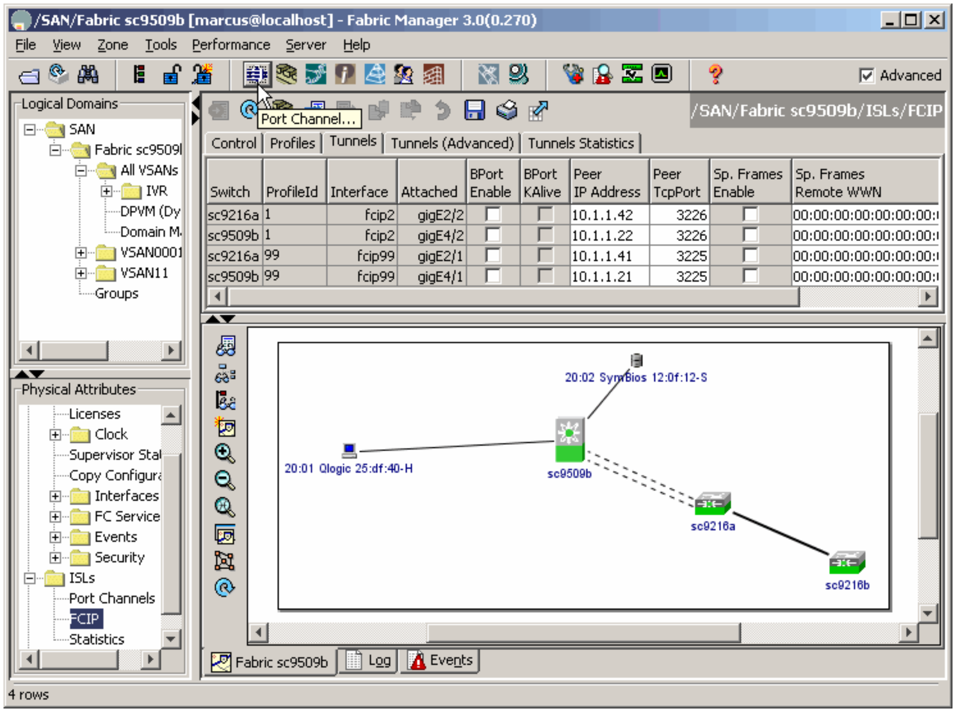
sc9509b,fcip2 <-> sc9216a,fcip2, 1 Gb, TE, VSAN 1

4 rows

Figure 4-109 The created FCIP tunnel is displayed in Fabric Manager

4.7.3 Creating a PortChannel on FCIP tunnels

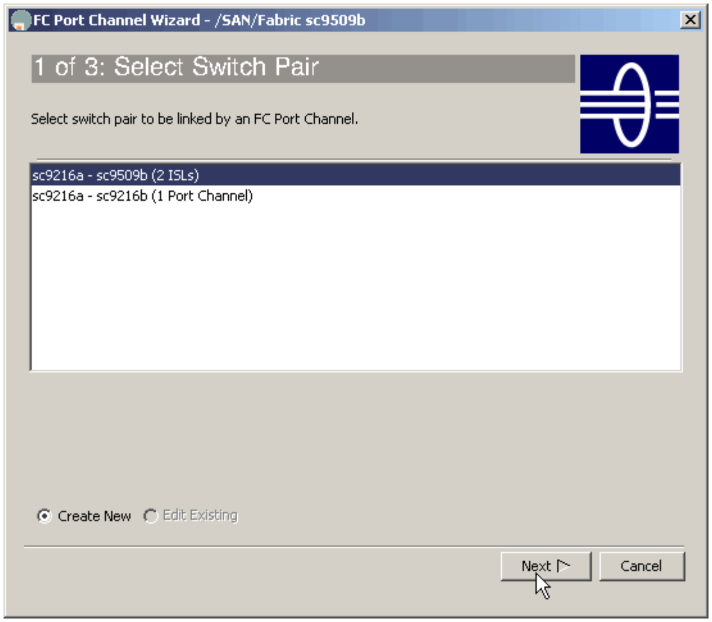
Now we show how to create a PortChannel on the FCIP tunnel using the GUI. We start the PortChannel wizard as shown in Figure 4-110.


/SAN/Fabric sc9509b [marcus@localhost] - Fabric Manager 3.0(0.270)
File View Zone Tools Performance Server Help
Advanced
Port Channel...
/SAN/Fabric sc9509b/ISLs/FCIP
Control Profiles Tunnels Tunnels (Advanced) Tunnels Statistics
Logical Domains
SAN
Fabric sc9509l
All VSANs
IVR
DPVM (Dy
Domain M.
VSAN0001
VSAN11
Groups
Physical Attributes
Licenses
Clock
Supervisor Stat
Copy Configura
Interfaces
FC Service
Events
Security
ISLs
Port Channels
FCIP
Statistics
20:02 SymBios 12:0f:12-S
20:01 Qlogic 25:df:40-H
sc9509b
sc9216a
sc9216b
Fabric sc9509b
Log
Events
4 rows

Switch	ProfileId	Interface	Attached	BPort Enable	BPort KAlive	Peer IP Address	Peer TcpPort	Sp. Frames Enable	Sp. Frames Remote WWN
sc9216a	1	fcip2	gigE2/2	☐	☐	10.1.1.42	3226	☐	00:00:00:00:00:00:00:
sc9509b	1	fcip2	gigE4/2	☐	☐	10.1.1.22	3226	☐	00:00:00:00:00:00:00:
sc9216a	99	fcip99	gigE2/1	☐	☐	10.1.1.41	3225	☐	00:00:00:00:00:00:00:
sc9509b	99	fcip99	gigE4/1	☐	☐	10.1.1.21	3225	☐	00:00:00:00:00:00:00:

Figure 4-110 Starting the Port Channel wizard

In Figure 4-111 we select the switch pair.


FC Port Channel Wizard - /SAN/Fabric sc9509b
1 of 3: Select Switch Pair

Select switch pair to be linked by an FC Port Channel.

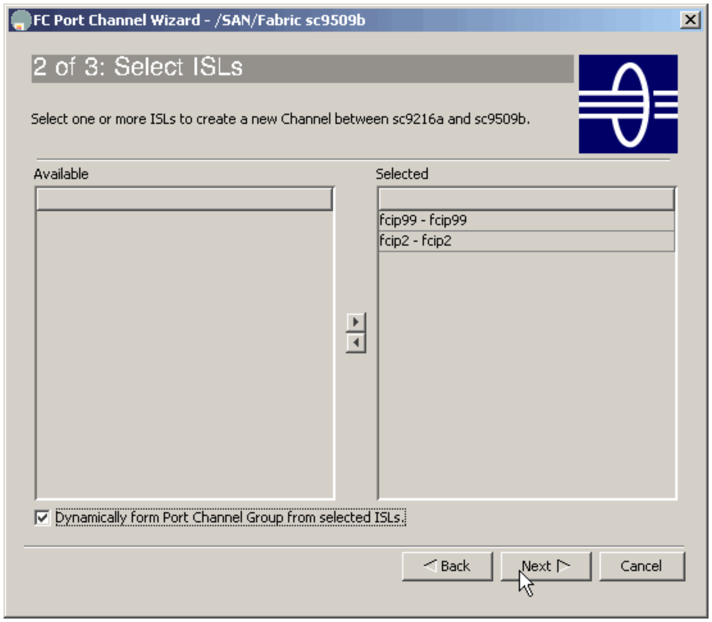
sc9216a - sc9509b (2 ISLs)
sc9216a - sc9216b (1 Port Channel)

● Create New ○ Edit Existing

Next
Cancel

Figure 4-111 Select switch pair

In Figure 4-112 we select the ISLs.


FC Port Channel Wizard - /SAN/Fabric sc9509b
2 of 3: Select ISLs

Select one or more ISLs to create a new Channel between sc9216a and sc9509b.

Available
Selected

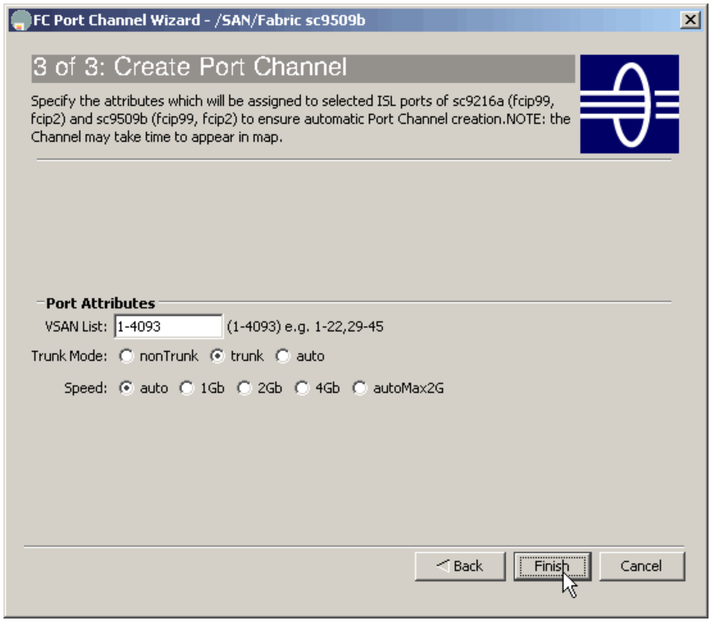
fcip99 - fcip99
fcip2 - fcip2

☑ Dynamically form Port Channel Group from selected ISLs.

Back
Next
Cancel

Figure 4-112 Selecting ISLs

In Figure 4-113 we create the PortChannel.


FC Port Channel Wizard - /SAN/Fabric sc9509b

3 of 3: Create Port Channel

Specify the attributes which will be assigned to selected ISL ports of sc9216a (fcip99, fcip2) and sc9509b (fcip99, fcip2) to ensure automatic Port Channel creation.NOTE: the Channel may take time to appear in map.

Port Attributes

VSAN List: 1-4093 (1-4093) e.g. 1-22,29-45

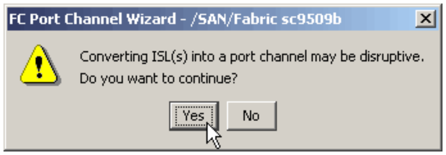
Trunk Mode: ○ nonTrunk ● trunk ○ auto

Speed: ● auto ○ 1Gb ○ 2Gb ○ 4Gb ○ autoMax2G

< Back
Finish
Cancel

Figure 4-113 Create Port Channel

In Figure 4-114 we confirm that we want to create the PortChannel.

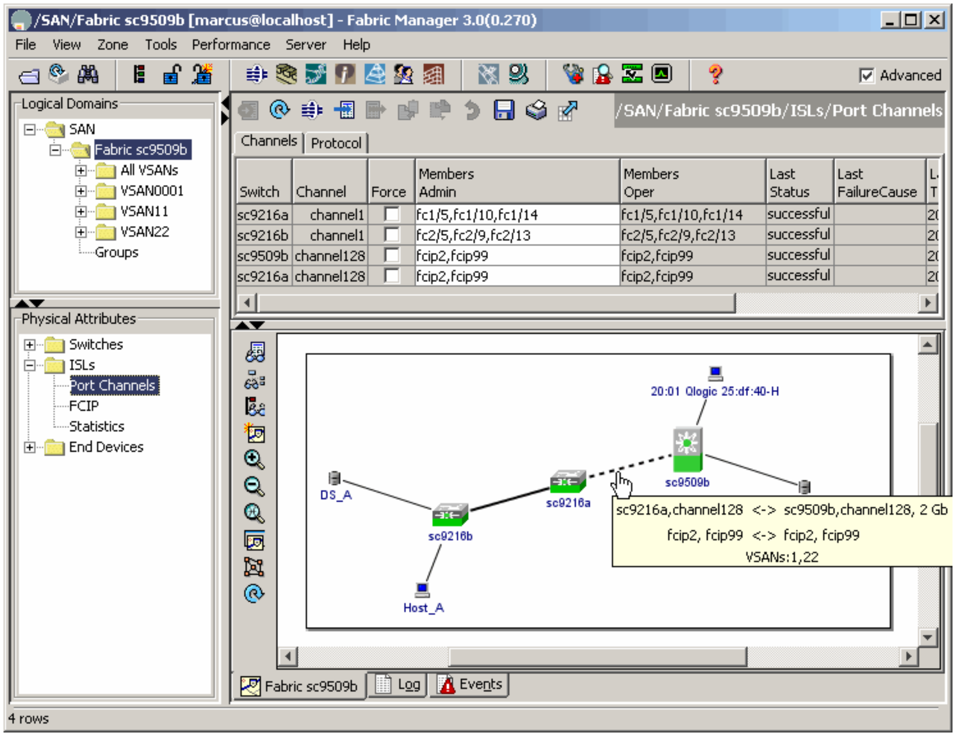

FC Port Channel Wizard - /SAN/Fabric sc9509b

Converting ISL(s) into a port channel may be disruptive.
Do you want to continue?

Yes
No

Figure 4-114 Confirm to create the PortChannel

In Figure 4-115 we show the created PortChannel.


/SAN/Fabric sc9509b [marcus@localhost] - Fabric Manager 3.0(0.270)
File View Zone Tools Performance Server Help
☑ Advanced
Logical Domains
SAN
Fabric sc9509b
All VSANs
VSAN0001
VSAN11
VSAN22
Groups
Physical Attributes
Switches
ISLs
Port Channels
FCIP
Statistics
End Devices
/SAN/Fabric sc9509b/ISLs/Port Channels
Channels
Protocol
20:01 Qlogic 25:df:40-H
DS_A
sc9216b
sc9216a
sc9509b
Host_A
Fabric sc9509b
Log
Events
4 rows

Switch	Channel	Force	Members Admin	Members Oper	Last Status	Last FailureCause	L T
sc9216a	channel1	☐	fc1/5,fc1/10,fc1/14	fc1/5,fc1/10,fc1/14	successful		2
sc9216b	channel1	☐	fc2/5,fc2/9,fc2/13	fc2/5,fc2/9,fc2/13	successful		2
sc9509b	channel128	☐	fcip2,fcip99	fcip2,fcip99	successful		2
sc9216a	channel128	☐	fcip2,fcip99	fcip2,fcip99	successful		2

sc9216a,channel128 <-> sc9509b,channel128, 2 Gb
fcip2, fcip99 <-> fcip2, fcip99
VSANs:1,22

Figure 4-115 The created Port Channel is displayed

4.7.4 iSCSI

The IPS module provides transparent SCSI routing by default. IP hosts using the iSCSI protocol can transparently access targets on the Fibre Channel network.

Note: We only show how to enable iSCSI and add an iSCSI initiator. The complexities of iSCSI will be covered in a future Redbooks publication.

Enabling iSCSI

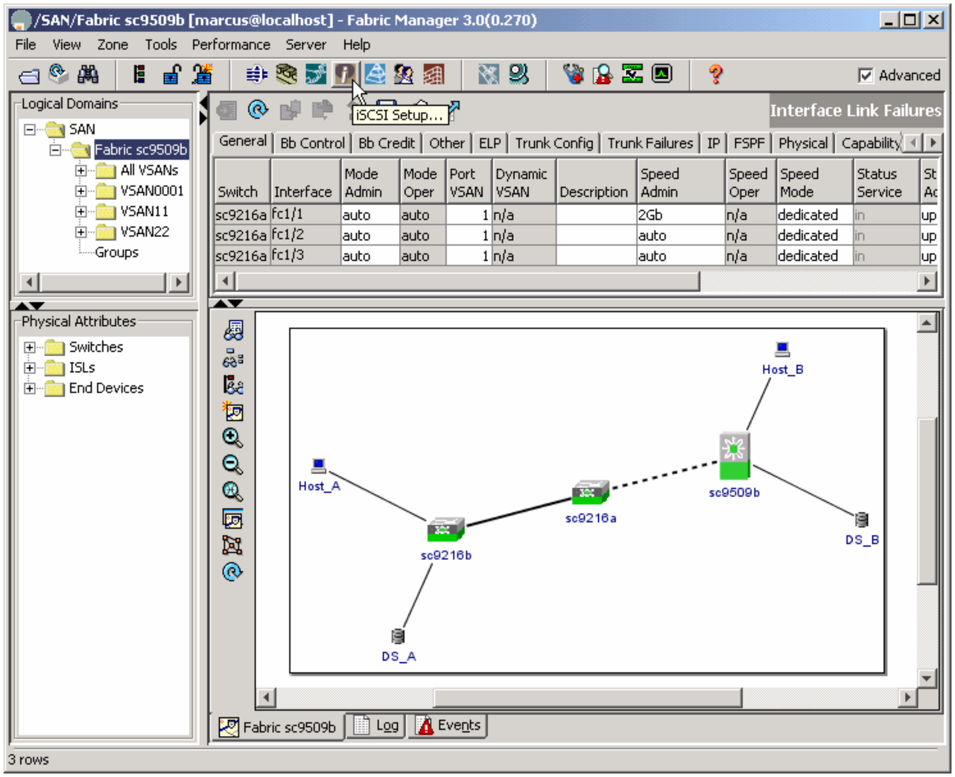
To begin configuring the iSCSI feature, you must explicitly enable iSCSI on the required switches in the fabric. By default, this feature is disabled in all switches in the Cisco MDS 9000 family. The configuration and verification commands for the iSCSI feature are only available when iSCSI is enabled on a switch. When you disable this feature, all related configurations are automatically discarded.

To enable iSCSI on a switch using Fabric Manager, follow these steps:

1. Choose **End Devices** > ISCSI from the Physical Attributes pane. You see the ISCSI tables in the Information pane.
2. Click the **Control** tab if it is not already displayed. You see the iSCSI enable status for all switches in the fabric that contain IPS ports.
3. Choose **Enable** from the Command column for each switch that you want to enable iSCSI on.
4. Click the **Apply Changes** icon to save these changes or click the **Undo Changes** icon to remove all changes without saving them.

Using the iSCSI wizard

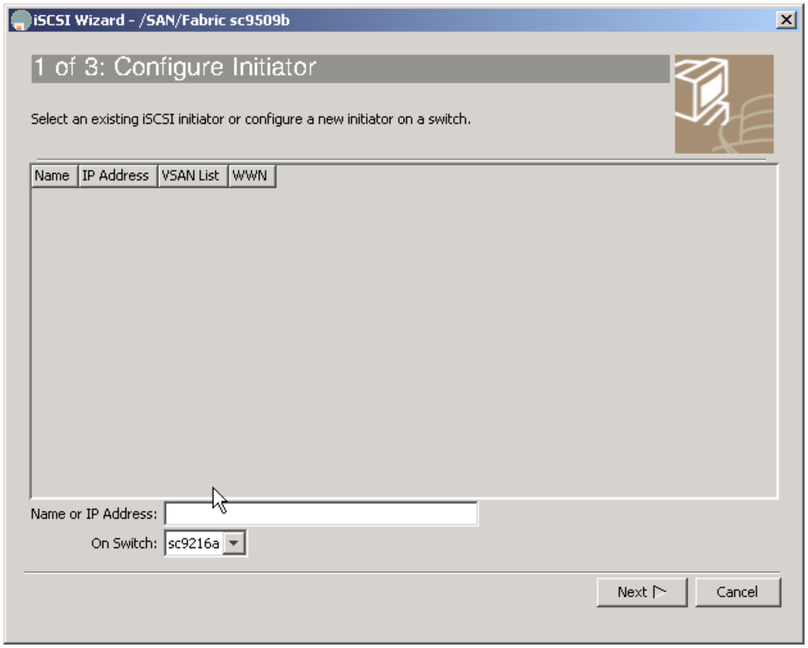
To use the iSCSI wizard in Fabric Manager, we select the iSCSI Setup Wizard icon, as shown in Figure 4-116.


/SAN/Fabric sc9509b [marcus@localhost] - Fabric Manager 3.0(0.270)
File
View
Zone
Tools
Performance
Server
Help
Advanced
iSCSI Setup...
Interface Link Failures
General
Bb Control
Bb Credit
Other
ELP
Trunk Config
Trunk Failures
IP
FSPF
Physical
Capability
Logical Domains
SAN
Fabric sc9509b
All VSANs
VSAN0001
VSAN11
VSAN22
Groups
Physical Attributes
Switches
ISLs
End Devices
Host_B
Host_A
sc9509b
sc9216a
sc9216b
DS_B
DS_A
Fabric sc9509b
Log
Events
3 rows

Switch	Interface	Mode Admin	Mode Oper	Port VSAN	Dynamic VSAN	Description	Speed Admin	Speed Oper	Speed Mode	Status Service	St Ac
sc9216a	fc1/1	auto	auto	1	n/a		2Gb	n/a	dedicated	in	up
sc9216a	fc1/2	auto	auto	1	n/a		auto	n/a	dedicated	in	up
sc9216a	fc1/3	auto	auto	1	n/a		auto	n/a	dedicated	in	up

Figure 4-116 iSCSI Setup Wizard icon

We now have to select an existing iSCSI initiator or add the iSCSI node name or IP address for a new iSCSI initiator. We select the switch for this iSCSI initiator as we are adding a new iSCSI initiator and click **Next**, as shown in Figure 4-117.


iSCSI Wizard - /SAN/Fabric sc9509b
1 of 3: Configure Initiator
Name
IP Address
VSAN List
WWN
Next
Cancel

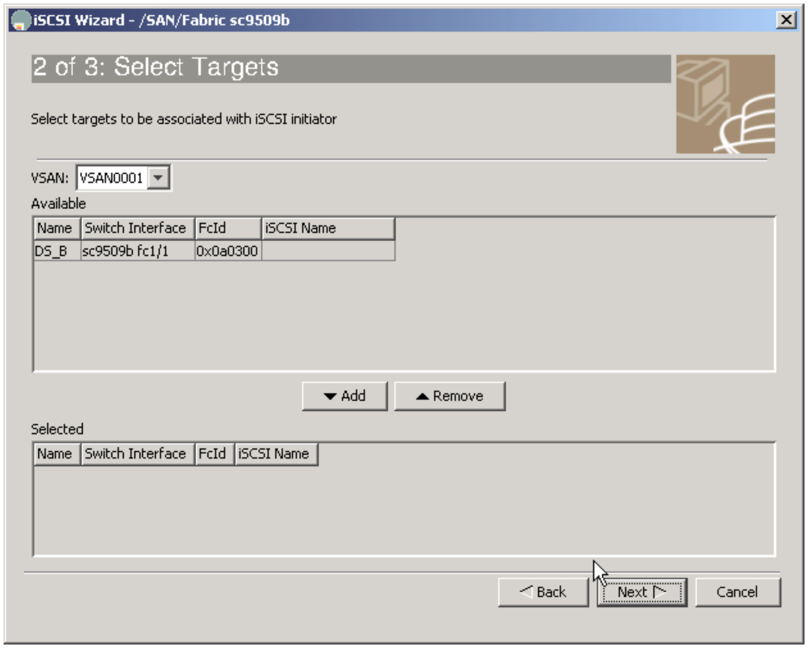
Select an existing iSCSI initiator or configure a new initiator on a switch.

Name or IP Address:

On Switch: sc9216a

Figure 4-117 iSCSI Configure Initiator

We then select the VSAN and targets to associate with this iSCSI initiator, as shown in Figure 4-118, and click **Next**.


iSCSI Wizard - /SAN/Fabric sc9509b
Add
Remove
Back
Next
Cancel

2 of 3: Select Targets

Select targets to be associated with iSCSI initiator

VSAN: VSAN0001

Available

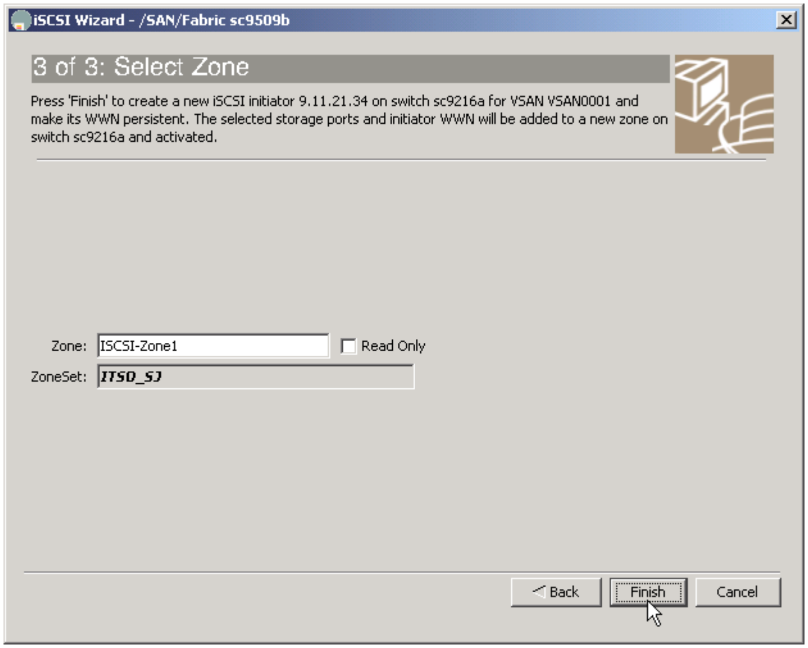
Name	Switch Interface	FcId	iSCSI Name
DS_B	sc9509b fc1/1	0x0a0300	

Selected

Name	Switch Interface	FcId	iSCSI Name

Figure 4-118 iSCSI Select Targets

We set the zone name for this new iSCSI zone and optionally check the **Read Only** check box, as shown in Figure 4-119.



iSCSI Wizard - /SAN/Fabric sc9509b

3 of 3: Select Zone

Press 'Finish' to create a new iSCSI initiator 9.11.21.34 on switch sc9216a for VSAN VSAN0001 and make its WWN persistent. The selected storage ports and initiator WWN will be added to a new zone on switch sc9216a and activated.

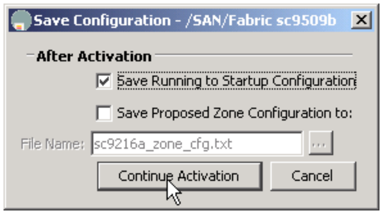
Zone: ISCSI-Zone1 ☐ Read Only

ZoneSet: ITSO_SJ

< Back
Finish
Cancel

Figure 4-119 iSCSI Select Zone

We are presented with the options as shown in Figure 4-120.



Save Configuration - /SAN/Fabric sc9509b
After Activation

☑ Save Running to Startup Configuration

☐ Save Proposed Zone Configuration to:

File Name: sc9216a_zone_cfg.txt

...
Continue Activation
Cancel

Figure 4-120 iSCSI Save Configuration

We have now created the iSCSI initiator.

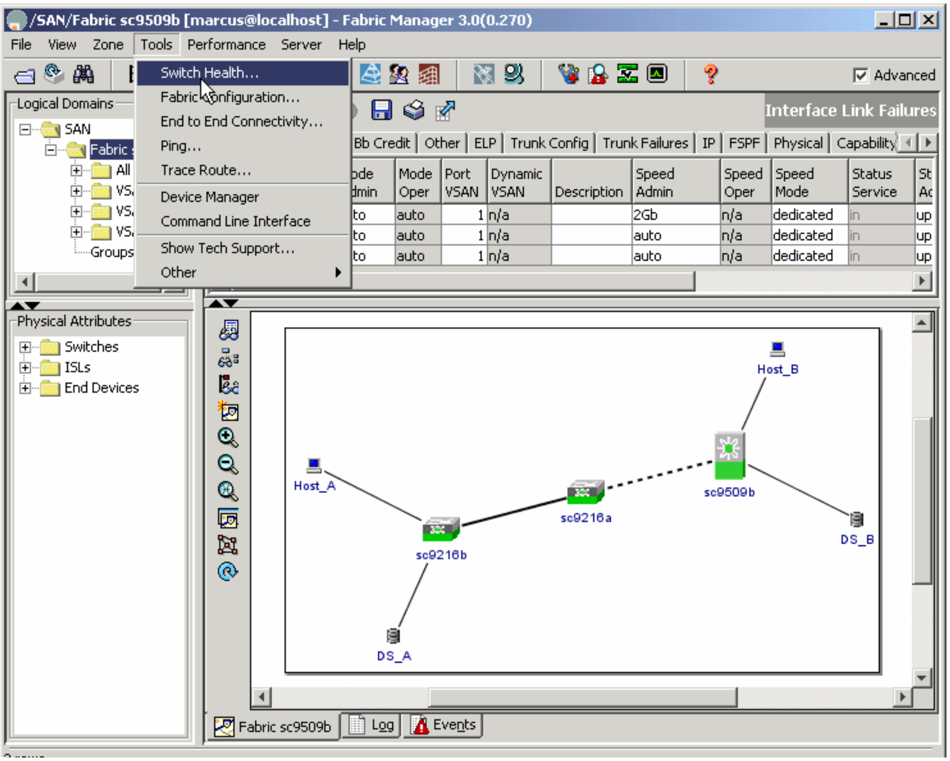
4.8 Fabric Manager analysis tools

FM has several tools that can be used to monitor the health of the fabric, status of individual switches, test end to end connectivity of devices, and monitor ISL performance. We discuss the following tools in this topic:

- Switch Health Analysis
- Fabric Configuration Analysis
- End to End Connectivity Analysis
- FC Ping
- FC Traceroute

4.8.1 Switch Health Analysis

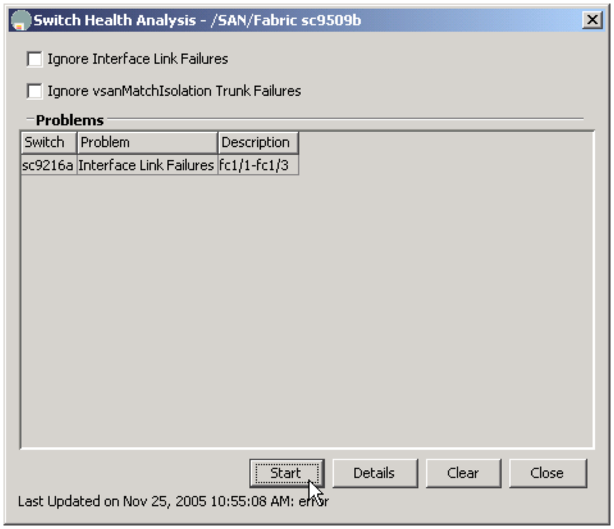
The Switch Health tool performs a check on the status of the components on each switch in the fabric. We start this tool by selecting **Tools** → **Switch Health** from the FM menu bar as shown in Figure 4-121.


/SAN/Fabric sc9509b [marcus@localhost] - Fabric Manager 3.0(0.270)
File
View
Zone
Tools
Performance
Server
Help
Switch Health...
Fabric Configuration...
End to End Connectivity...
Ping...
Trace Route...
Device Manager
Command Line Interface
Show Tech Support...
Other
☑ Advanced
Interface Link Failures
Logical Domains
SAN
Fabric
All
VS
VS
VS
Groups
Bb Credit
Other
ELP
Trunk Config
Trunk Failures
IP
FSPF
Physical
Capability
Physical Attributes
Switches
ISLs
End Devices
Host_B
Host_A
sc9509b
sc9216a
sc9216b
DS_B
DS_A
Fabric sc9509b
Log
Events

ode dmin	Mode Oper	Port VSAN	Dynamic VSAN	Description	Speed Admin	Speed Oper	Speed Mode	Status Service	St Ac
to	auto	1	n/a		2Gb	n/a	dedicated	in	up
to	auto	1	n/a		auto	n/a	dedicated	in	up
to	auto	1	n/a		auto	n/a	dedicated	in	up

Figure 4-121 Selecting Switch Health

This displays the Fabric Manager - Switch Health Analysis window shown in Figure 4-122. Select **Start** to begin the analysis. When it has performed its analysis, the results are shown under the Problems heading.



Switch Health Analysis - /SAN/Fabric sc9509b

☐ Ignore Interface Link Failures

☐ Ignore vsanMatchIsolation Trunk Failures

Problems

Switch	Problem	Description
sc9216a	Interface Link Failures	fc1/1-fc1/3

Last Updated on Nov 25, 2005 10:55:08 AM: error

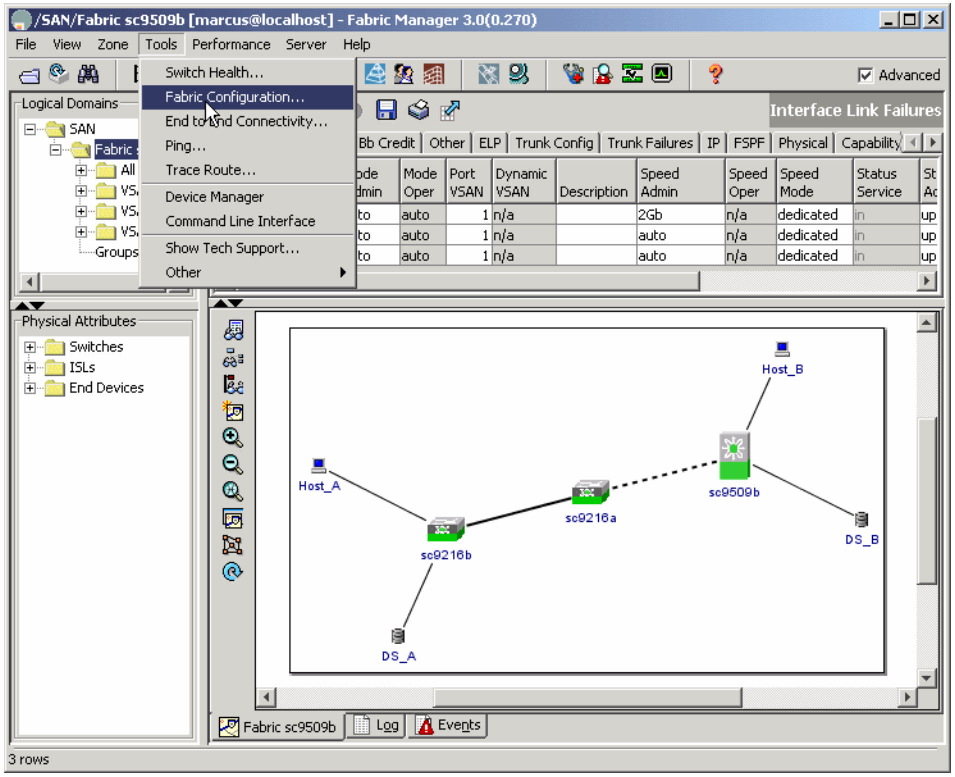
Figure 4-122 Switch Health Analysis output

We can highlight specific problems and select the **Details** button to get further details.

4.8.2 Fabric Configuration Analysis

The Fabric Configuration Analysis tool lets you analyze the configuration of a switch by comparing the current configuration to another switch or to an individual configuration file. You can save a switch configuration to a file and then compare all switches against the configuration in the file.

We this tool by selecting **Tools** → **Fabric Configuration** from the FM menu bar as shown in Figure 4-123.

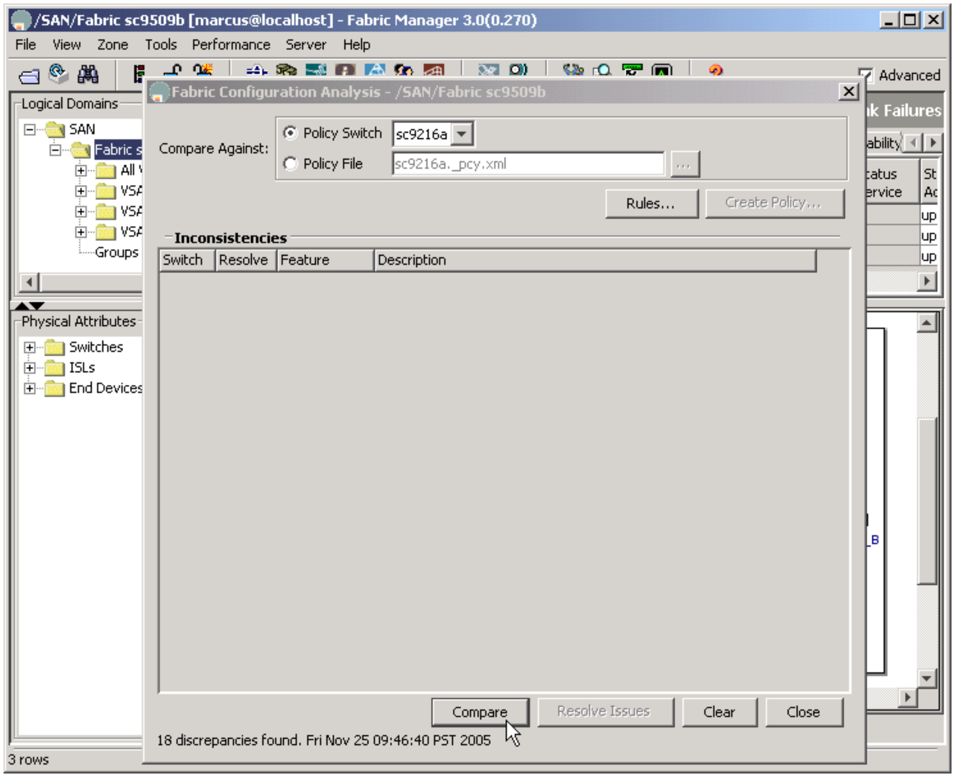


/SAN/Fabric sc9509b [marcus@localhost] - Fabric Manager 3.0(0.270)
File
View
Zone
Tools
Performance
Server
Help
Switch Health...
Fabric Configuration...
End to End Connectivity...
Ping...
Trace Route...
Device Manager
Command Line Interface
Show Tech Support...
Other
Advanced
Interface Link Failures
Bb Credit
Other
ELP
Trunk Config
Trunk Failures
IP
FSPF
Physical
Capability
Logical Domains
SAN
Fabric
All
VS
VS
VS
Groups
Physical Attributes
Switches
ISLs
End Devices
Host_B
Host_A
sc9216a
sc9509b
sc9216b
DS_B
DS_A
Fabric sc9509b
Log
Events
3 rows

ode dmin	Mode Oper	Port VSAN	Dynamic VSAN	Description	Speed Admin	Speed Oper	Speed Mode	Status Service	St Ac
to	auto	1	n/a		2Gb	n/a	dedicated	in	up
to	auto	1	n/a		auto	n/a	dedicated	in	up
to	auto	1	n/a		auto	n/a	dedicated	in	up

Figure 4-123 Selecting Fabric Configuration analysis

Figure 4-124 shows the Fabric Configuration Analysis window, and we selected Compare to perform the check. In this example we have two switches in the fabric: sc9509b and sc9216a. We used the 9216 switch as the policy switch, so when we selected **Compare**, the configuration of the 9216 was checked against the configuration of the 9509 and inconsistencies were found.

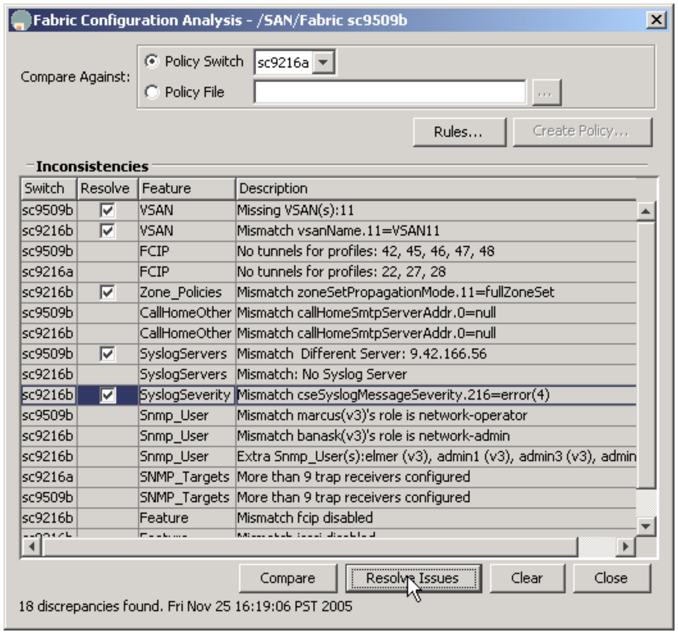

/SAN/Fabric sc9509b [marcus@localhost] - Fabric Manager 3.0(0.270)
File View Zone Tools Performance Server Help
Advanced
Logical Domains
SAN
Fabric s
Groups
Physical Attributes
Switches
ISLs
End Devices
3 rows
Fabric Configuration Analysis - /SAN/Fabric sc9509b
Rules...
Create Policy...
Inconsistencies
Switch
Resolve
Feature
Description
Compare
Resolve Issues
Clear
Close

Compare Against: ● Policy Switch sc9216a ○ Policy File sc9216a._pcy.xml

18 discrepancies found. Fri Nov 25 09:46:40 PST 2005

Figure 4-124 Comparing configuration

Figure 4-125 shows that we might be able to resolve some of the errors (indicated by the check mark). We can press the Resolve Issues button to attempt to do so.


Fabric Configuration Analysis - /SAN/Fabric sc9509b
Compare Against:
Rules...
Create Policy...
Compare
Resolve Issues
Clear
Close

● Policy Switch sc9216a
○ Policy File

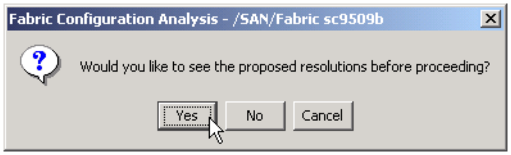
Inconsistencies

Switch	Resolve	Feature	Description
sc9509b	☑	VSAN	Missing VSAN(s):11
sc9216b	☑	VSAN	Mismatch vsanName.11=VSAN11
sc9509b		FCIP	No tunnels for profiles: 42, 45, 46, 47, 48
sc9216a		FCIP	No tunnels for profiles: 22, 27, 28
sc9216b	☑	Zone_Policies	Mismatch zoneSetPropagationMode.11=fullZoneSet
sc9509b		CallHomeOther	Mismatch callHomeSmtpServerAddr.0=null
sc9216b		CallHomeOther	Mismatch callHomeSmtpServerAddr.0=null
sc9509b	☑	SyslogServers	Mismatch Different Server: 9.42.166.56
sc9216b		SyslogServers	Mismatch: No Syslog Server
sc9216b	☑	SyslogSeverity	Mismatch cseSyslogMessageSeverity.216=error(4)
sc9509b		Snmp_User	Mismatch marcus(v3)'s role is network-operator
sc9216b		Snmp_User	Mismatch banask(v3)'s role is network-admin
sc9216b		Snmp_User	Extra Snmp_User(s):elmer (v3), admin1 (v3), admin3 (v3), admin
sc9216a		SNMP_Targets	More than 9 trap receivers configured
sc9509b		SNMP_Targets	More than 9 trap receivers configured
sc9216b		Feature	Mismatch fcip disabled

18 discrepancies found. Fri Nov 25 16:19:06 PST 2005

Figure 4-125 Fabric Configuration Analysis - resolve issues

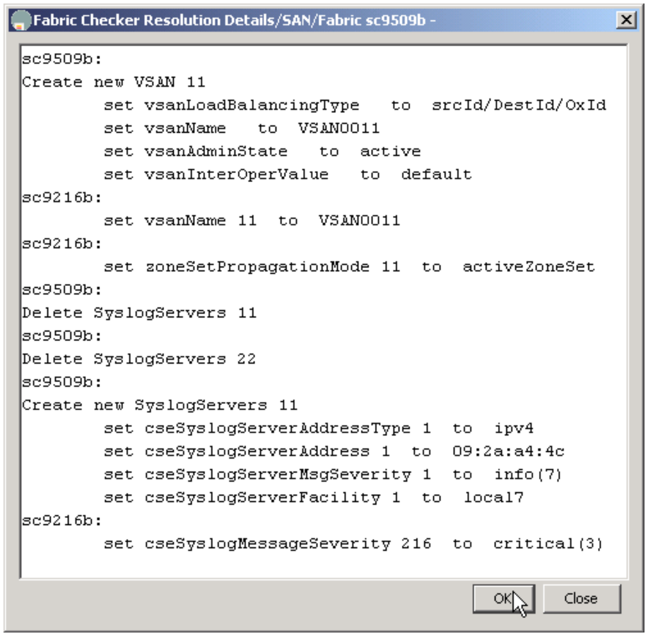
We are asked if we would like to see the proposed resolutions, as shown in Figure 4-126.


Fabric Configuration Analysis - /SAN/Fabric sc9509b
Yes
No
Cancel

Would you like to see the proposed resolutions before proceeding?

Figure 4-126 Proposed resolutions

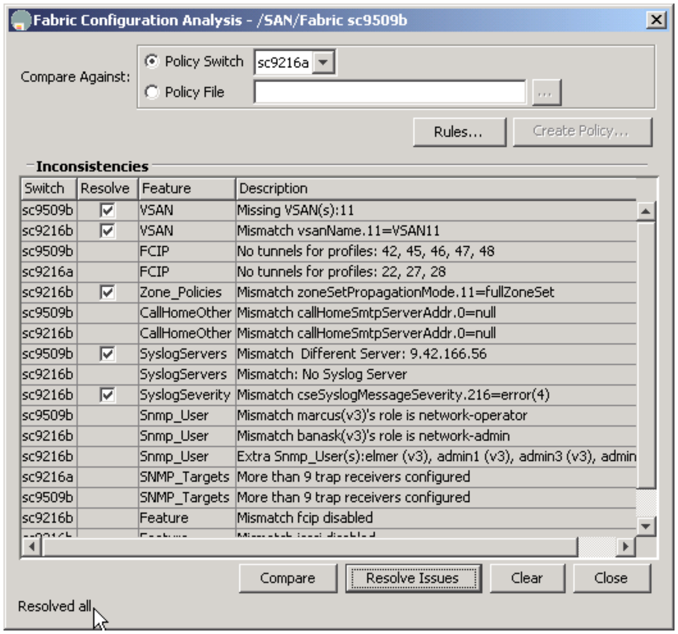
We are presented with the output as shown in Figure 4-127.



```
sc9509b:
Create new VSAN 11
        set vsanLoadBalancingType   to  srcId/DestId/OxId
        set vsanName   to  VSAN0011
        set vsanAdminState   to  active
        set vsanInterOperValue   to  default
sc9216b:
        set vsanName 11  to  VSAN0011
sc9216b:
        set zoneSetPropagationMode 11  to  activeZoneSet
sc9509b:
Delete SyslogServers 11
sc9509b:
Delete SyslogServers 22
sc9509b:
Create new SyslogServers 11
        set cseSyslogServerAddressType 1  to  ipv4
        set cseSyslogServerAddress 1  to  09:2a:a4:4c
        set cseSyslogServerMsgSeverity 1  to  info(7)
        set cseSyslogServerFacility 1  to  local7
sc9216b:
        set cseSyslogMessageSeverity 216  to  critical(3)
```

Figure 4-127 Fabric Checker Resolution Details

If we click **OK**, the details are applied as shown in Figure 4-128.



Compare Against: ● Policy Switch sc9216a ○ Policy File

Switch	Resolve	Feature	Description
sc9509b	☑	VSAN	Missing VSAN(s):11
sc9216b	☑	VSAN	Mismatch vsanName.11=VSAN11
sc9509b		FCIP	No tunnels for profiles: 42, 45, 46, 47, 48
sc9216a		FCIP	No tunnels for profiles: 22, 27, 28
sc9216b	☑	Zone_Policies	Mismatch zoneSetPropagationMode.11=fullZoneSet
sc9509b		CallHomeOther	Mismatch callHomeSmtpServerAddr.0=null
sc9216b		CallHomeOther	Mismatch callHomeSmtpServerAddr.0=null
sc9509b	☑	SyslogServers	Mismatch Different Server: 9.42.166.56
sc9216b		SyslogServers	Mismatch: No Syslog Server
sc9216b	☑	SyslogSeverity	Mismatch cseSyslogMessageSeverity.216=error(4)
sc9509b		Snmp_User	Mismatch marcus(v3)'s role is network-operator
sc9216b		Snmp_User	Mismatch banask(v3)'s role is network-admin
sc9216b		Snmp_User	Extra Snmp_User(s):elmer (v3), admin1 (v3), admin3 (v3), admin
sc9216a		SNMP_Targets	More than 9 trap receivers configured
sc9509b		SNMP_Targets	More than 9 trap receivers configured
sc9216b		Feature	Mismatch fcip disabled

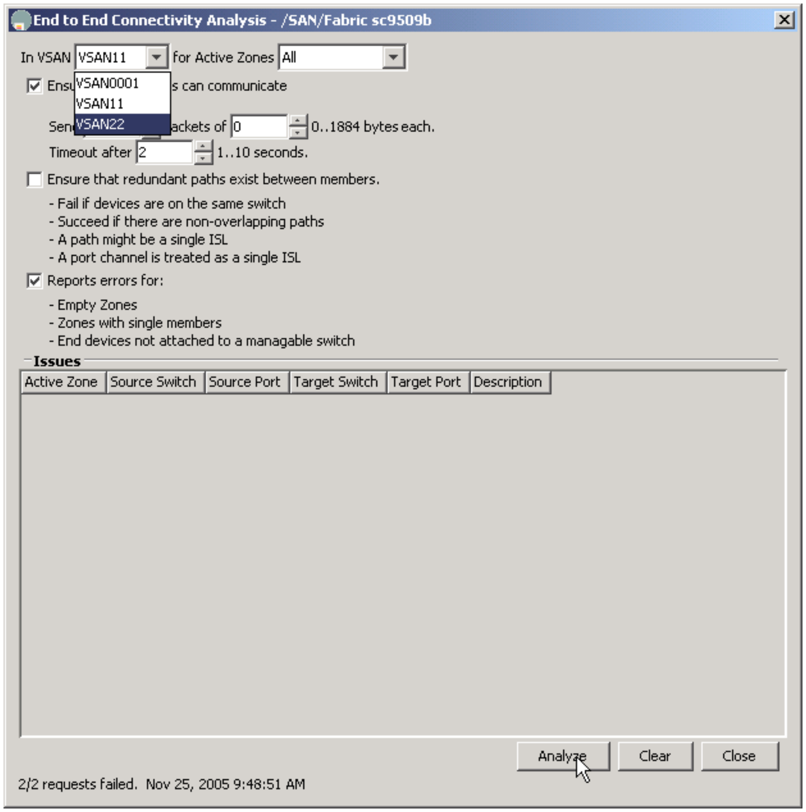
Resolved all

Figure 4-128 Displaying the successful resolutions

4.8.3 End to End Connectivity Analysis

You can use the End to End Connectivity analysis tool to determine connectivity and routes among devices within the switch fabric. The tool checks to see that every pair of end devices can talk to each other using a **`ping`** test and by determining if they are in the same VSAN, or in the same active zone. This tool uses versions of **`ping`** and **`traceroute`** commands modified for Fibre Channel networks.

We can start this tool by selecting **Tools** → **End to End** Connectivity from the FM menu bar and we are presented with the screen as shown in Figure 4-129.


End to End Connectivity Analysis - /SAN/Fabric sc9509b

In VSAN VSAN11 for Active Zones All

☑ Ensu s can communicate

Sen ackets of 0 0..1884 bytes each.

Timeout after 2 1..10 seconds.

☐ Ensure that redundant paths exist between members.

- Fail if devices are on the same switch
- Succeed if there are non-overlapping paths
- A path might be a single ISL
- A port channel is treated as a single ISL

☑ Reports errors for:

- Empty Zones
- Zones with single members
- End devices not attached to a managable switch

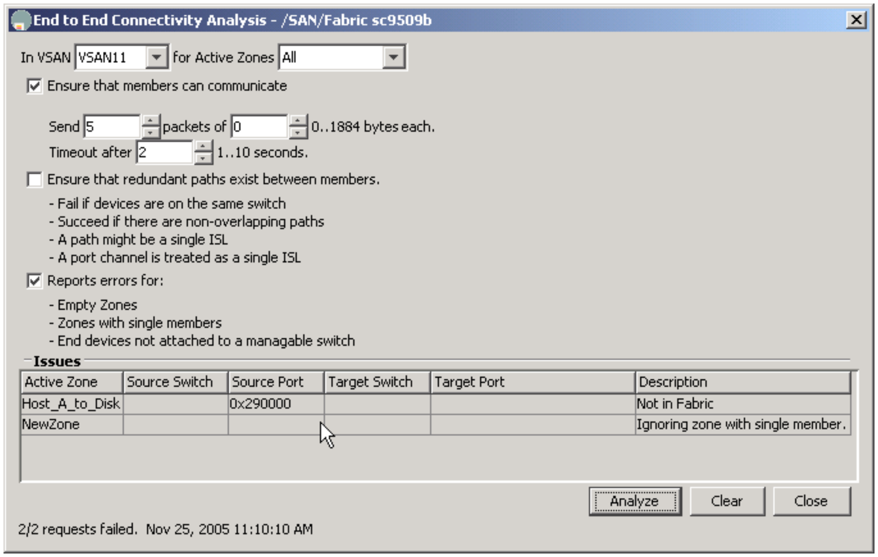
Issues

Active Zone	Source Switch	Source Port	Target Switch	Target Port	Description

2/2 requests failed. Nov 25, 2005 9:48:51 AM

Figure 4-129 End to End Connectivity Analysis

In Figure 4-130 we have selected that for VSAN 11 in All Zones that we would like to ensure that all members can communicate. The Issues are shown at the bottom of the screen.



End to End Connectivity Analysis - /SAN/Fabric sc9509b

In VSAN VSAN11 for Active Zones All

☑ Ensure that members can communicate

Send 5 packets of 0 0..1884 bytes each.
Timeout after 2 1..10 seconds.

☐ Ensure that redundant paths exist between members.

- Fail if devices are on the same switch
- Succeed if there are non-overlapping paths
- A path might be a single ISL
- A port channel is treated as a single ISL

☑ Reports errors for:

- Empty Zones
- Zones with single members
- End devices not attached to a managable switch

Issues

Active Zone	Source Switch	Source Port	Target Switch	Target Port	Description
Host_A_to_Disk		0x290000			Not in Fabric
NewZone					Ignoring zone with single member.

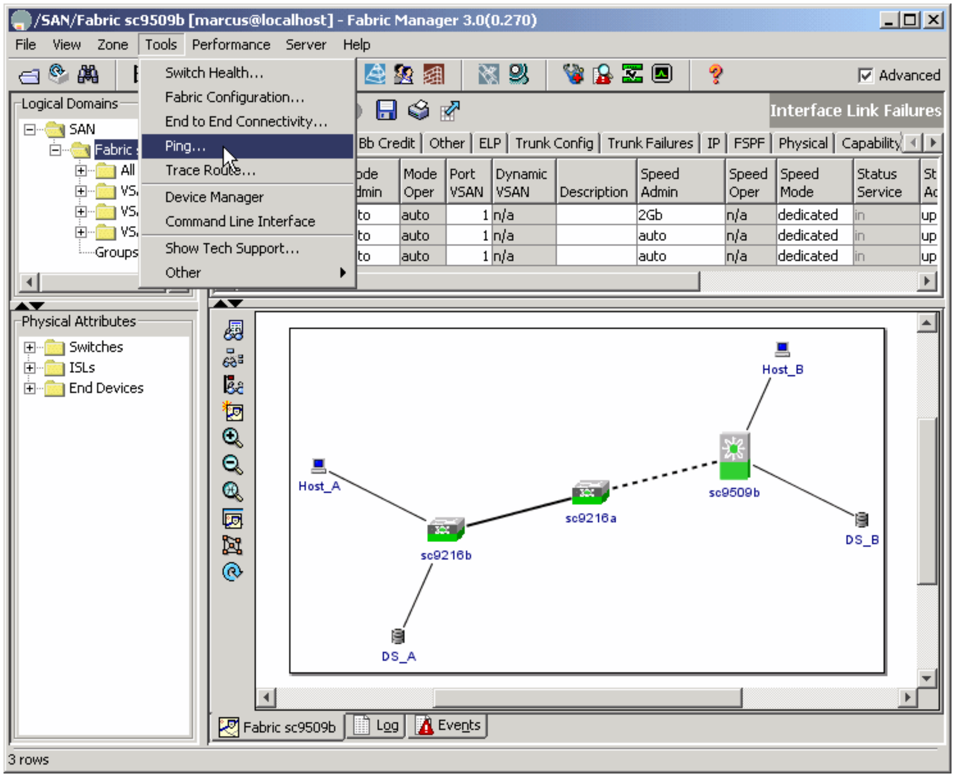
2/2 requests failed. Nov 25, 2005 11:10:10 AM

Figure 4-130 End to End Connectivity Analysis

4.8.4 FC Ping

FM also provides an FC Ping tool that allows you to check connectivity to end devices. The Ping consists of a Port Login (PLOGI), followed by an ECHO extended link service command sourced with the switch FCID FF.FC.XX where XX is the domain ID of the switch for that VSAN.

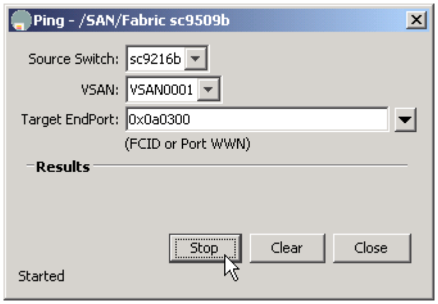
To use the tool, we select **Tools** → **Ping** from the FM menu bar and we are presented with the screen as shown in Figure 4-131.


/SAN/Fabric sc9509b [marcus@localhost] - Fabric Manager 3.0(0.270)
File
View
Zone
Tools
Performance
Server
Help
Switch Health...
Fabric Configuration...
End to End Connectivity...
Ping...
Trace Route...
Device Manager
Command Line Interface
Show Tech Support...
Other
☑ Advanced
Interface Link Failures
Logical Domains
SAN
Fabric s
All
VS.
VS.
VS.
Groups
Bb Credit
Other
ELP
Trunk Config
Trunk Failures
IP
FSPF
Physical
Capability
Physical Attributes
Switches
ISLs
End Devices
Host_B
Host_A
sc9509b
sc9216a
sc9216b
DS_B
DS_A
Fabric sc9509b
Log
Events
3 rows

ode dmin	Mode Oper	Port VSAN	Dynamic VSAN	Description	Speed Admin	Speed Oper	Speed Mode	Status Service	St Ac
to	auto	1	n/a		2Gb	n/a	dedicated	in	up
to	auto	1	n/a		auto	n/a	dedicated	in	up
to	auto	1	n/a		auto	n/a	dedicated	in	up

Figure 4-131 Selecting Ping

We then see the FM Ping window as shown in Figure 4-132. At this point we can select which switch we want to source the ping from (sc9216b), which VSAN to use, and the end port we want to FC Ping.


Ping - /SAN/Fabric sc9509b
(FCID or Port WWN)
Results
Stop
Clear
Close

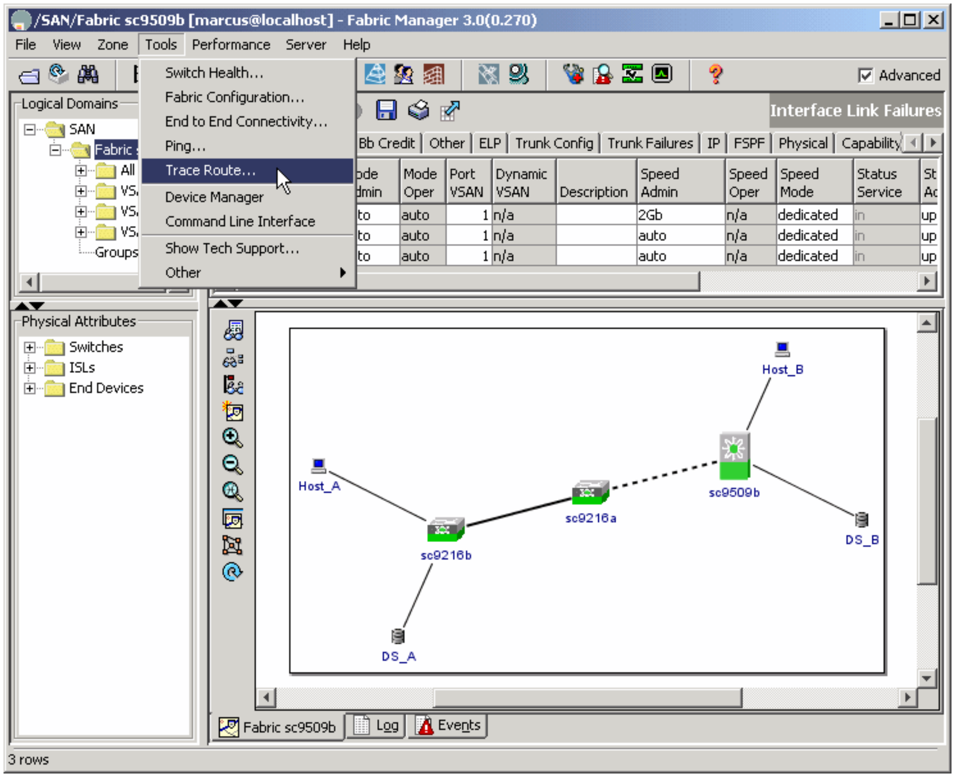
Source Switch: sc9216b
VSAN: VSAN0001
Target EndPort: 0x0a0300
Started

Figure 4-132 Ping window

When the Ping completes, it tells us whether it has been successful or not.

4.8.5 FC Traceroute

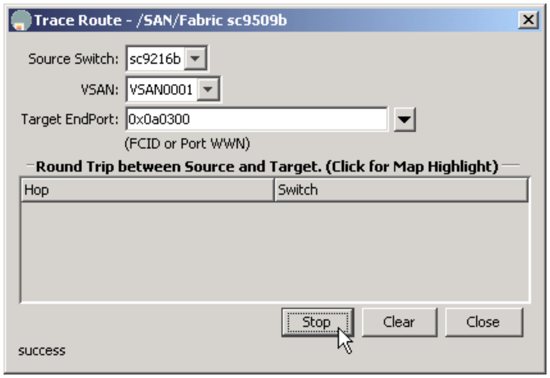
The MDS SAN-OS also provides a modified FC Traceroute tool as an aid in determining end to end connectivity. To access this tool from FM we select **Tools** → **Trace Route** from the FM menu bar as shown in Figure 4-133.


/SAN/Fabric sc9509b [marcus@localhost] - Fabric Manager 3.0(0.270)
File
View
Zone
Tools
Performance
Server
Help
Switch Health...
Fabric Configuration...
End to End Connectivity...
Ping...
Trace Route...
Device Manager
Command Line Interface
Show Tech Support...
Other
Advanced
Logical Domains
SAN
Fabric
All
VS
VS
VS
Groups
Interface Link Failures
Bb Credit
Other
ELP
Trunk Config
Trunk Failures
IP
FSPF
Physical
Capability
Physical Attributes
Switches
ISLs
End Devices
Host_B
Host_A
sc9509b
sc9216a
sc9216b
DS_B
DS_A
Fabric sc9509b
Log
Events
3 rows

ode dmin	Mode Oper	Port VSAN	Dynamic VSAN	Description	Speed Admin	Speed Oper	Speed Mode	Status Service	St Ac
to	auto	1	n/a		2Gb	n/a	dedicated	in	up
to	auto	1	n/a		auto	n/a	dedicated	in	up
to	auto	1	n/a		auto	n/a	dedicated	in	up

Figure 4-133 Selecting Trace Route

We are presented with the screen shown in Figure 4-134, where we can select the route we want to trace.



Source Switch: sc9216b
VSAN: VSAN0001
Target EndPort: 0x0a0300
(FCID or Port WWN)

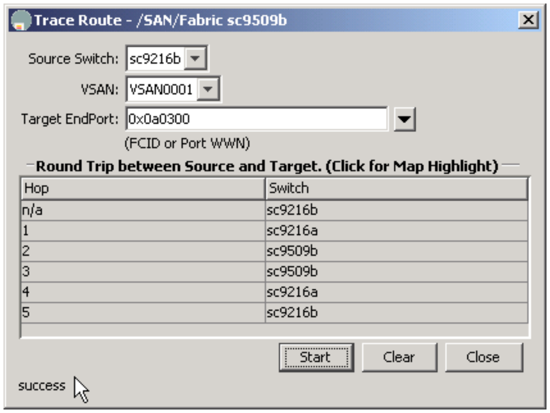
Round Trip between Source and Target. (Click for Map Highlight)

Hop	Switch

success

Figure 4-134 Trace Route success

In Figure 4-135 we can see the possible routes.



Source Switch: sc9216b
VSAN: VSAN0001
Target EndPort: 0x0a0300
(FCID or Port WWN)

Round Trip between Source and Target. (Click for Map Highlight)

Hop	Switch
n/a	sc9216b
1	sc9216a
2	sc9509b
3	sc9509b
4	sc9216a
5	sc9216b

success

Figure 4-135 Trace Route possible routes

4.8.6 Show Tech Support

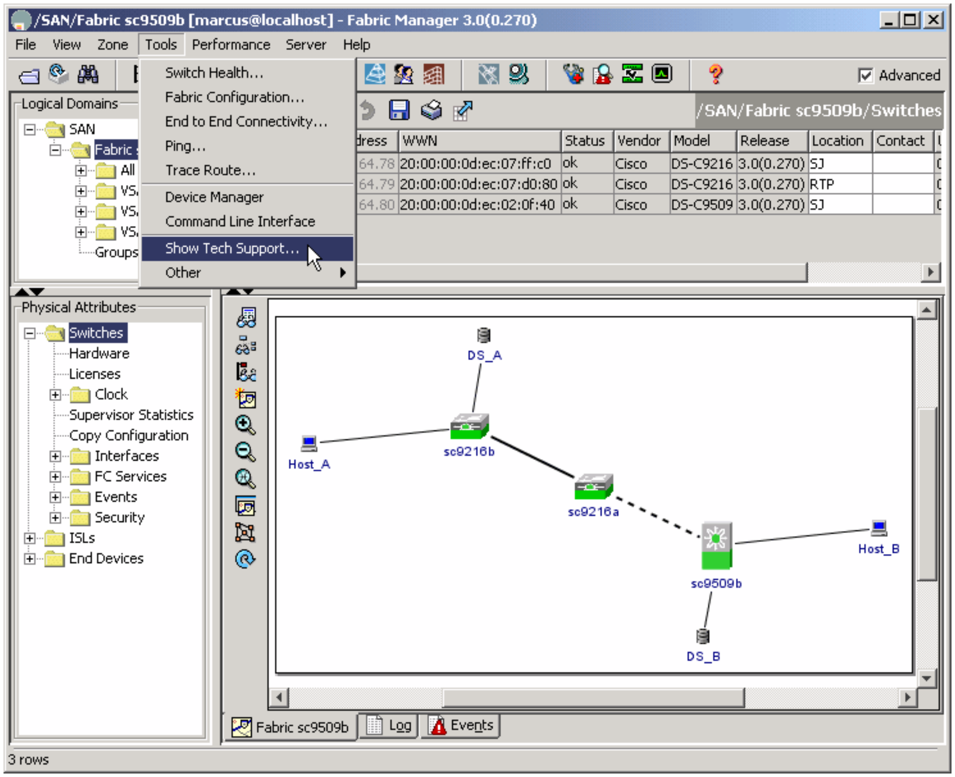
The Show Tech Support output is useful when collecting a large amount of information about your switch for troubleshooting purposes. The output of this command can be provided to technical support representatives when reporting a problem. It displays the output of several **`show`** commands at once. The output from this varies depending on your configuration.

> **Note:** Use the **`show tech-support`** command in EXEC mode to display general information about the switch when reporting a problem.

The output is the equivalent of entering these commands:

- `show version`
- `show environment`
- `show module`
- `show hardware`
- `show running-config`
- `show interface`
- `show accounting log`
- `show process`
- `show process log`
- `show processes log details`
- `show flash`

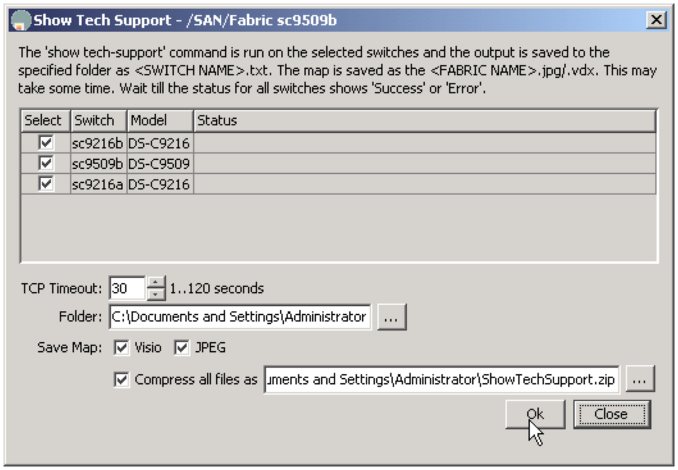
In Figure 4-136 we show how to launch Show Tech Support.


/SAN/Fabric sc9509b [marcus@localhost] - Fabric Manager 3.0(0.270)
File
View
Zone
Tools
Performance
Server
Help
Switch Health...
Fabric Configuration...
End to End Connectivity...
Ping...
Trace Route...
Device Manager
Command Line Interface
Show Tech Support...
Other
Advanced
/SAN/Fabric sc9509b/Switches
Logical Domains
SAN
Fabric
All
VS
VS
VS
Groups
Physical Attributes
Switches
Hardware
Licenses
Clock
Supervisor Statistics
Copy Configuration
Interfaces
FC Services
Events
Security
ISLs
End Devices
DS_A
Host_A
sc9216b
sc9216a
sc9509b
Host_B
DS_B
Fabric sc9509b
Log
Events
3 rows

dress	WWN	Status	Vendor	Model	Release	Location	Contact
64.78	20:00:00:0d:ec:07:ff:c0	ok	Cisco	DS-C9216	3.0(0.270)	SJ	
64.79	20:00:00:0d:ec:07:d0:80	ok	Cisco	DS-C9216	3.0(0.270)	RTP	
64.80	20:00:00:0d:ec:02:0f:40	ok	Cisco	DS-C9509	3.0(0.270)	SJ	

Figure 4-136 Launching Show Tech Support

In Figure 4-137 we show the switches we want to capture data for, and how and where we want to save the output.



Show Tech Support - /SAN/Fabric sc9509b

The 'show tech-support' command is run on the selected switches and the output is saved to the specified folder as <SWITCH NAME>.txt. The map is saved as the <FABRIC NAME>.jpg/.vdx. This may take some time. Wait till the status for all switches shows 'Success' or 'Error'.

Select	Switch	Model	Status
☑	sc9216b	DS-C9216	
☑	sc9509b	DS-C9509	
☑	sc9216a	DS-C9216	

TCP Timeout: 30 1..120 seconds

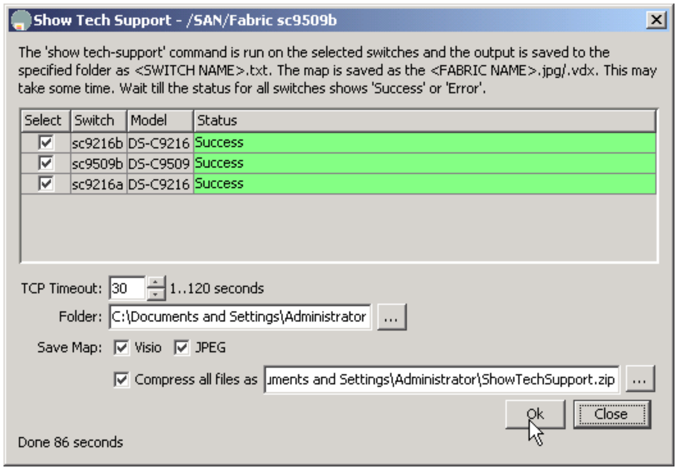
Folder: C:\Documents and Settings\Administrator

Save Map: ☑ Visio ☑ JPEG

☑ Compress all files as ıments and Settings\Administrator\ShowTechSupport.zip

Figure 4-137 Selecting switches

In Figure 4-138 we can see that we have met with success.



Show Tech Support - /SAN/Fabric sc9509b

The 'show tech-support' command is run on the selected switches and the output is saved to the specified folder as <SWITCH NAME>.txt. The map is saved as the <FABRIC NAME>.jpg/.vdx. This may take some time. Wait till the status for all switches shows 'Success' or 'Error'.

Select	Switch	Model	Status
☑	sc9216b	DS-C9216	Success
☑	sc9509b	DS-C9509	Success
☑	sc9216a	DS-C9216	Success

TCP Timeout: 30 1..120 seconds

Folder: C:\Documents and Settings\Administrator

Save Map: ☑ Visio ☑ JPEG

☑ Compress all files as ıments and Settings\Administrator\ShowTechSupport.zip

Done 86 seconds

Figure 4-138 Successful results

We can see where and how we have saved the output.

4.8.7 Cisco Fabric Analyzer

Fibre Channel protocol analyzers capture, decode, and analyze frames and ordered sets on a link. Existing Fibre Channel analyzers can capture traffic at wire rate speed. They are expensive and support limited frame decoding. Also, to snoop traffic, the existing analyzers disrupt the traffic on the link while the analyzer is inserted into the link. With the Cisco Fabric Analyzer you can capture Fibre Channel control traffic from a switch and decode it without having to disrupt any connectivity, and without having to be local to the point of analysis. The Cisco Fibre Channel protocol analyzer is based on two popular public-domain software applications:

- libpcap:

  http://www.tcpdump.org

- Ethereal:

  http://www.ethereal.com

Note: The Cisco Fabric Analyzer is useful in capturing and decoding control traffic, not data traffic. It is suitable for control path captures, and is not intended for high-speed data path captures.

The Cisco Fabric Analyzer consists of two separate components:

- Software that runs on the Cisco MDS 9000 family switch and supports two modes of capture:
  - A text-based analyzer that supports local capture and decodes captured frames
  - A daemon that supports remote capture
- GUI-based client that runs on a host that supports libpcap such as Windows or Linux and communicates with the remote capture daemon in a Cisco MDS 9000 family switch.

Local Text-Based Capture

This component is a command-line driven text-based interface that captures traffic to and from the supervisor module in a Cisco MDS 9000 family switch. It is a fully functional decoder that is useful for quick debug purposes or for use when the remote capture daemon is not enabled. Additionally, because this tool is accessed from within the Cisco MDS 9000 family switch, it is protected by the roles-based policy that limits access in each switch.

Remote Capture Daemon

This daemon is the server end of the remote capture component. The Ethereal analyzer running on a host is the client end. They communicate with each other using the Remote Capture Protocol (RPCAP). RPCAP uses two endpoints, a TCP-based control connection and a TCP or UDP-based data connection based on TCP (default) or UDP.

The control connection is used to remotely control the captures (start or stop the capture, or specify capture filters). Remote capture can only be performed to explicitly configured hosts. This technique prevents an unauthorized machine in the network from snooping on the control traffic in the network.

RPCAP supports two setup connection modes based on firewall restrictions:

- **Passive mode (default):** The configured host initiates connection to the switch. Multiple hosts can be configured to be in passive mode and multiple hosts can be connected and receive remote captures at the same time.
- **Active mode:** The switch initiates the connection to a configured host — one host at a time.

Using capture filters, you can limit the amount of traffic that is actually sent to the client. Capture filters are specified at the client end—on Ethereal, not on the switch.

GUI-based client

The Ethereal software runs on a host, such as a PC or workstation, and communicates with the remote capture daemon. This software is available in the public domain from:

`http://www.ethereal.com`

The Ethereal GUI front-end supports a rich interface such as a colorized display, graphical assists in defining filters, and specific frame searches. These features are documented on Ethereal's Web site. While remote capture through Ethereal supports capturing and decoding Fibre Channel frames from a Cisco MDS 9000 family switch, the host running Ethereal does not require a Fibre Channel connection to the switch. The remote capture daemon running on the switch sends the captured frames over the out-of-band Ethernet management port. This capability allows you to capture and decode Fibre Channel frames from your desktop or laptop (mobile computer).

4.8.8 Monitoring network traffic using SPAN

The Cisco MDS 9000 family provides a feature called the switch port analyzer (SPAN). The SPAN or SD_Ports allow us to monitor network traffic through the Fibre Channel interface.

Traffic through any Fibre Channel interface can be replicated to a special port called the SPAN destination port. Any Fibre Channel port in a switch can be configured as an SD_Port. When an interface is in SD_Port mode, it cannot be used for normal data traffic. You can attach a Fibre Channel analyzer to the SD_Port to monitor SPAN traffic.

Note: RSPAN has all the features of SPAN plus support for source ports and destination ports distributed across multiple switches, allowing remote monitoring of multiple switches across your network.

The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. The SPAN traffic from the sources, which cannot be in the RSPAN VLAN, is switched to the RSPAN VLAN and then forwarded to destination ports configured in the RSPAN VLAN.

The traffic type for sources (ingress, egress, or both) in an RSPAN session can be different in different source switches, but is the same for all sources in each source switch for each RSPAN session. Do not configure any ports in an RSPAN VLAN except those selected to carry RSPAN traffic. Learning is disabled on the RSPAN VLAN.

SD_Ports do not receive frames, they only transmit a copy of the SPAN source traffic. The SPAN feature is non-intrusive and does not affect switching of network traffic for any SPAN source port.

Illustrated in Figure 4-139 is an overview of the SPAN port.

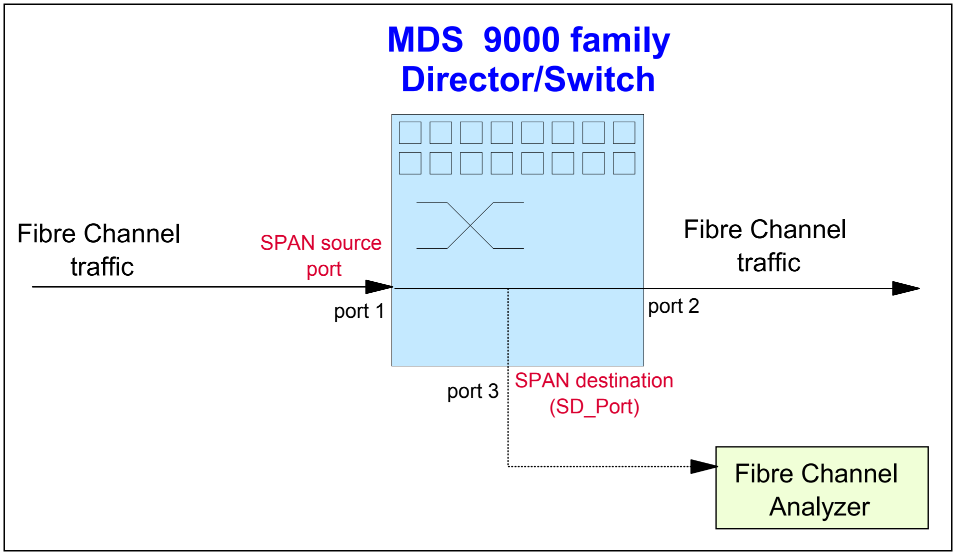

MDS 9000 family
Director/Switch
Fibre Channel traffic
SPAN source port
port 1
Fibre Channel traffic
port 2
port 3
SPAN destination (SD_Port)
Fibre Channel Analyzer

Figure 4-139 SPAN destination ports

SPAN sources

A SPAN source is the interface from which traffic can be monitored. You can also specify a VSAN as a SPAN source, in which case, all supported interfaces in the specified VSAN are included as SPAN sources. You can choose the SPAN traffic in the ingress direction, the egress direction, or both directions, for any source interface.

- **Ingress source (rx):** Traffic entering the switch fabric through this source is spanned or copied to the SD_Port, as shown in Figure 4-140.

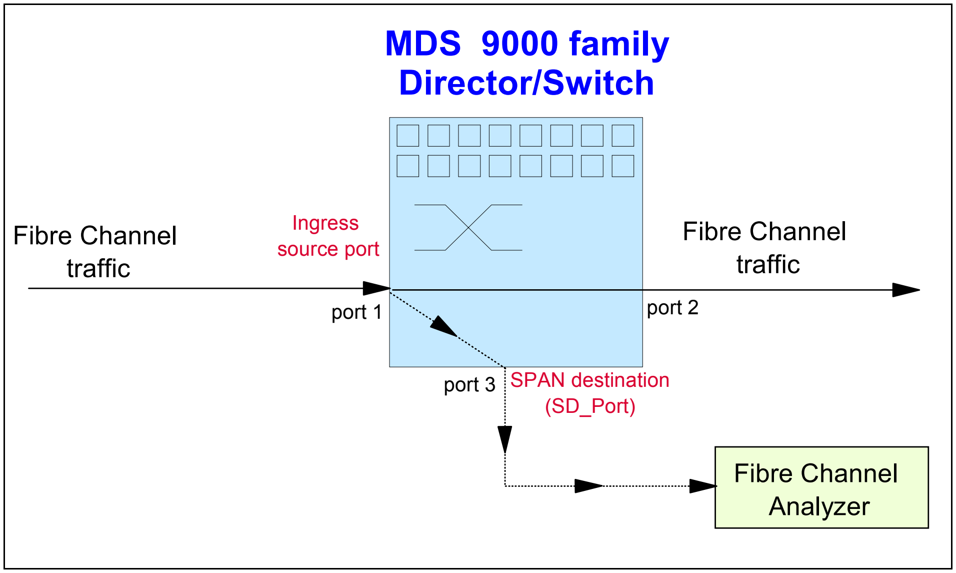

MDS 9000 family
Director/Switch
Fibre Channel traffic
Ingress source port
port 1
Fibre Channel traffic
port 2
port 3
SPAN destination (SD_Port)
Fibre Channel Analyzer

Figure 4-140 SD_Port for incoming traffic (ingress direction)

- **Egress source (tx):** Traffic exiting the switch fabric through this source interface is spanned or copied to the SD_Port, as shown in Figure 4-141.

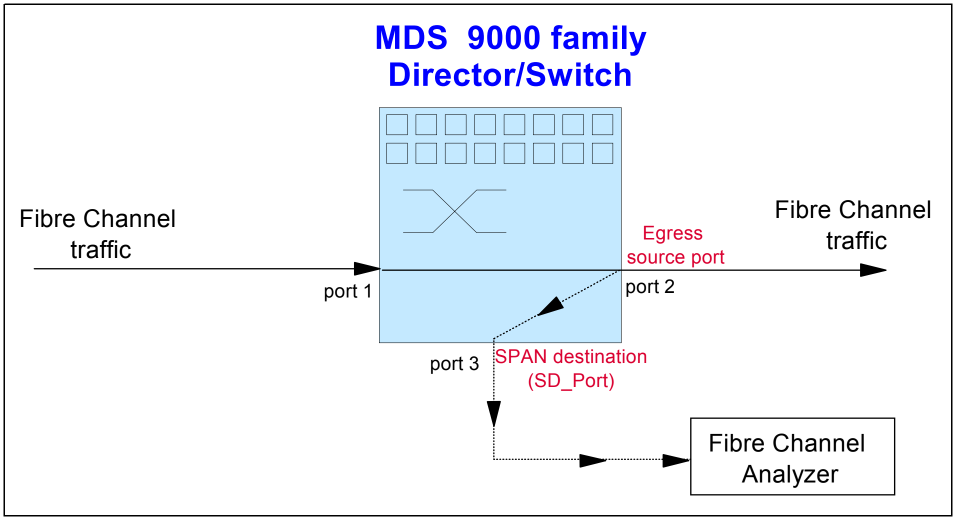

MDS 9000 family
Director/Switch
Fibre Channel traffic
port 1
Egress source port
port 2
Fibre Channel traffic
port 3
SPAN destination (SD_Port)
Fibre Channel Analyzer

Figure 4-141 SD_Port for outgoing traffic (egress direction)

Allowed source interface types

The SPAN feature is available for the following interface types:

- Physical ports:
  - F_Ports, FL_Ports, TE_Ports, E_Ports, and TL_Ports.
- Interface sup-fc0 (traffic to and from the supervisor):
  - The Fibre Channel traffic from the supervisor module to the switch fabric, through the sup-fc0 interface, is called ingress traffic. It is spanned when sup-fc0 is chosen as an ingress source port.
  - The Fibre Channel traffic from the switch fabric to the supervisor module, through the sup-fc0 interface, is called egress traffic. It is spanned when sup-fc0 is chosen as an egress source port.
- PortChannels:
  - All ports in the PortChannel are included and spanned as sources.
  - You cannot specify individual ports in a PortChannel as SPAN sources. Previously-configured SPAN-specific interface information is discarded.

VSAN as a SPAN source

When a VSAN as a source is specified, then all physical ports and PortChannels in that VSAN are included as SPAN sources. A TE_Port is included only when the port VSAN of the TE_Port matches the source VSAN. A TE_Port is excluded even if the configured allowed VSAN list can have the source VSAN, but the port VSAN is different.

Guidelines for configuring VSANs as a source

The following guidelines apply when configuring VSANs as a source:

- Traffic on all interfaces included in a source VSAN is spanned only in the ingress direction.
- When a VSAN is specified as a source, you will not be able to perform interface-level configuration on the interfaces that are included in the VSAN. Previously-configured SPAN-specific interface information is discarded.
- If an interface in a VSAN is configured as a SPAN source, you will not be able to configure that VSAN as a source. You must first remove the existing SPAN configurations on such interfaces before configuring VSAN as a source.
- Interfaces are only included as sources when the port VSAN matches the source VSAN.

SPAN sessions

Each SPAN session represents an association of one destination with a set of source(s) along with various other parameters that you specify to monitor the network traffic. One destination can be used by one or more SPAN sessions. You can configure up to 16 SPAN sessions in a switch. Each session can have several source ports and one destination port.

To activate a SPAN session, at least one source and the SD_Port must be up and functioning. Otherwise, traffic will not be directed to the SD_Port.

To temporarily deactivate (suspend) a SPAN session use the **`suspend`** command in the SPAN submode. The traffic monitoring is stopped during this time. You can reactivate the SPAN session using the **`no suspend`** command.

Specifying filters

You can perform VSAN-based filtering to selectively monitor network traffic on specified VSANs. You can apply this VSAN filter to the selected source or to all sources in a session. Only traffic in the selected VSANs is spanned when you configure VSAN filters. You can specify two types of VSAN filters:

- **Interface level filters:** You can apply VSAN filters for a specified TE_Port or trunking PortChannel to filter traffic using one of three options — the ingress direction, the egress direction, or both directions.
- **Session filters:** This option filters all sources in the specified session. These filters are bi-directional and apply to all sources configured in the session.

Guidelines for specifying filters

The following guidelines apply to SPAN filters:

- Specify filters in either the ingress direction, or in the egress direction, or in both directions.
- PortChannel filters are applied to all ports in the PortChannel.
- If no filters are specified, the traffic from all active VSANs for that interface is spanned.
- The effective filter on a port is the intersection (filters common to both) of interface filters and session filters.
- While you can specify any arbitrary VSAN filters in an interface, traffic can only be monitored on the port VSAN or on allowed-active VSANs in that interface.
- When you configure VSAN as a source, that VSAN is implicitly applied as an interface filter to all sources included in the specified VSAN.

SD_Port characteristics

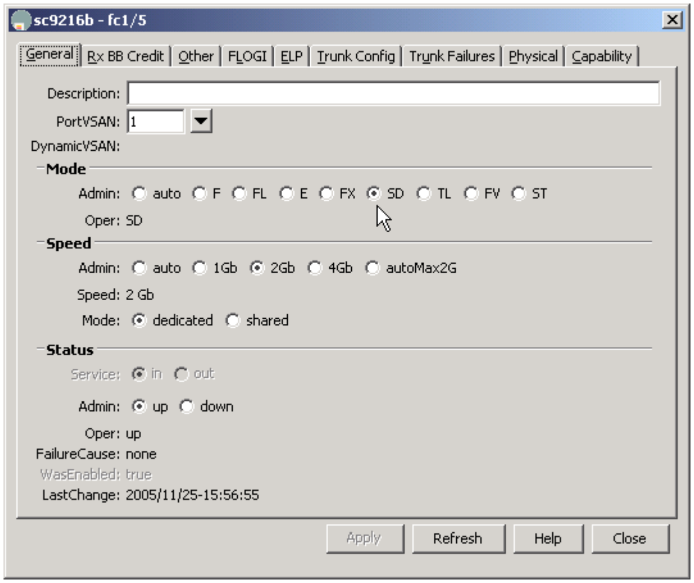
An SD_Port has the following characteristics:

- It ignores buffer-to-buffer credits.
- It allows data traffic only in the egress (tx) direction.
- It does not require a device or an analyzer to be physically connected.
- It supports only 1 Gbps or 2 Gbps speeds. The auto speed option is not allowed.
- Multiple sessions can share the same destination ports.
- If the SD_Port is shut down, all shared sessions stop generating SPAN traffic.
- The port mode cannot be changed if it is being used for a SPAN session.
- The outgoing frames can be encapsulated in EISL format.
- The SD_Port does not have a port VSAN.

The following guidelines apply for a SPAN configuration:

- You can configure up to 16 SPAN sessions with multiple ingress (rx) sources.
- You can configure a maximum of three SPAN sessions with one egress (tx) port.
- In a 32 port switching module, you must configure the same session in all four ports in one port group. If you want, you can also configure only two or three ports in this unit.
- SPAN frames are dropped if the sum of the bandwidth of the sources exceeds the speed of the destination port.
- Frames dropped by a source port are not spanned.

In Figure 4-142 we show how to set FC1/5 as an SD port.


sc9216b - fc1/5

General
Rx BB Credit
Other
FLOGI
ELP
Trunk Config
Trunk Failures
Physical
Capability

Description:
PortVSAN: 1
DynamicVSAN:

Mode

Admin: ○ auto ○ F ○ FL ○ E ○ FX ● SD ○ TL ○ FV ○ ST
Oper: SD

Speed

Admin: ○ auto ○ 1Gb ● 2Gb ○ 4Gb ○ autoMax2G
Speed: 2 Gb
Mode: ● dedicated ○ shared

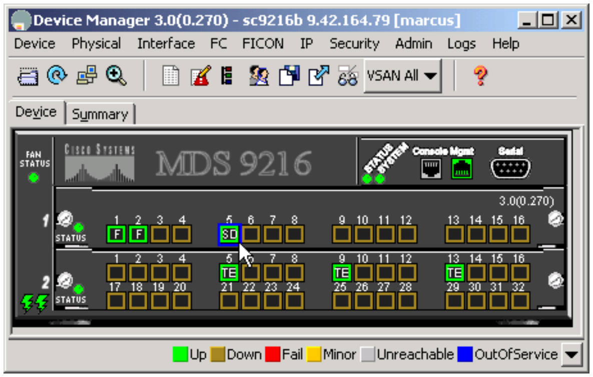
Status

Service: ● in ○ out
Admin: ● up ○ down
Oper: up
FailureCause: none
WasEnabled: true
LastChange: 2005/11/25-15:56:55

Apply
Refresh
Help
Close

Figure 4-142 Setting FC1/5 as SD

In Device Manager we can see that it is now an SD port, as shown in Figure 4-143.


Device Manager 3.0(0.270) - sc9216b 9.42.164.79 [marcus]

Device
Physical
Interface
FC
FICON
IP
Security
Admin
Logs
Help
VSAN All
Device
Summary
FAN STATUS
Cisco Systems
MDS 9216
STATUS SYSTEM
Console Mgmt
Serial
3.0(0.270)
1
2
STATUS
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
F F SD
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
TE TE TE
17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
🟩Up
🟫Down
🟥Fail
🟨Minor
⬜Unreachable
🟦OutOfService

Figure 4-143 FC1/5 is an SD port

4.8.9 System message logging

The system message logging software saves messages in a log file or directs the messages to other devices. This feature provides you with the following capabilities:

- It provides logging information for monitoring and troubleshooting
- It allows you to select the types of captured logging information.
- It allows you to select the destination server to forward the captured logging information.

By default, the switch logs normal but significant system messages to a log file and sends these messages to the system console. You can specify which system messages should be saved based on the type of facility and the severity level. Messages are time-stamped to enhance real-time debugging and management.

You can access logged system messages using the CLI or by saving them to a properly configured system message logging server. The switch software saves system messages in a file that can be configured to save up to 4 MB. You can monitor system messages remotely by accessing the switch through Telnet, SSH, or the console port, or by viewing the logs on a system message logging server.

Use the **`show logging`** command to display the current system message logging configuration. We show some examples of logging commands and, in the interests of brevity, we have omitted the output.

To display NVRM log contents:

- **`show logging nvram`**

To display the log file:

- **`show logging logfile`**

To display console logging status:

- **`show logging console`**

To display the logging facility:

- **`show logging level`**

To display logging information:

- **`show logging info`**

To display the last two lines of a log file:

- **`show logging last 2`**

To display switching module logging status:

- `show logging module`

To display monitor logging status:

- `show logging monitor`

To displays server information:

- `show logging server`

4.8.10 Call Home

Call Home provides e-mail-based notification of critical system events. A versatile range of message formats are available for optimal compatibility with pager services, standard e-mail, or XML-based automated parsing applications.

Common uses of this feature can include direct paging of a network support engineer, e-mail notification to a Network Operations Center, and utilization of Cisco AutoNotify services for direct case generation with the Technical Assistance Center.

The Call Home feature provides message throttling capabilities. Periodic inventory messages, port syslog messages and RMON alert messages are added to the list of deliverable Call Home messages. If required, you can also use the Cisco Fabric Services application to distribute the Call Home configuration to all other switches in the fabric.

4.9 FICON quickstart implementation

In this topic we discuss the basic steps to configuring s witch for FICON in both a switched point-to-point and cascaded configuration. We are using Fabric Manager and Device Manager to perform all configuration steps.

We discuss some basic FICON/mainframe steps that you have to perform. It is not our intent to show any of the steps on the mainframe, however we highlight the considerations.

4.10 Hardware Configuration Definition

An I/O configuration defines the hardware resources available to the operating system and the connections between these resources. The resources include:

- Channels
- ESCON/FICON Directors (switches)
- Control units
- Devices

You must define an I/O configuration to the operating system (software) and the channel subsystem (hardware). The Hardware Configuration Definition (HCD) element of z/OS combines hardware and software I/O configuration under a single interactive end-user interface. HCD also performs validation checking which helps to eliminate errors before you attempt to use the I/O configuration.

The output of HCD is an I/O definition file (IODF). An IODF is used to define multiple hardware and software configurations to the z/OS operating system. When you activate an IODF, HCD defines the I/O configuration to the channel subsystem and/or the operating system. With the HCD activate function or the **`MVS ACTIVATE`** operator command, you can make changes to the current configuration without having to perform an initial program load (IPL) the software or power-on reset (POR) the hardware. Making changes while the system is running is known as dynamic configuration or dynamic reconfiguration.

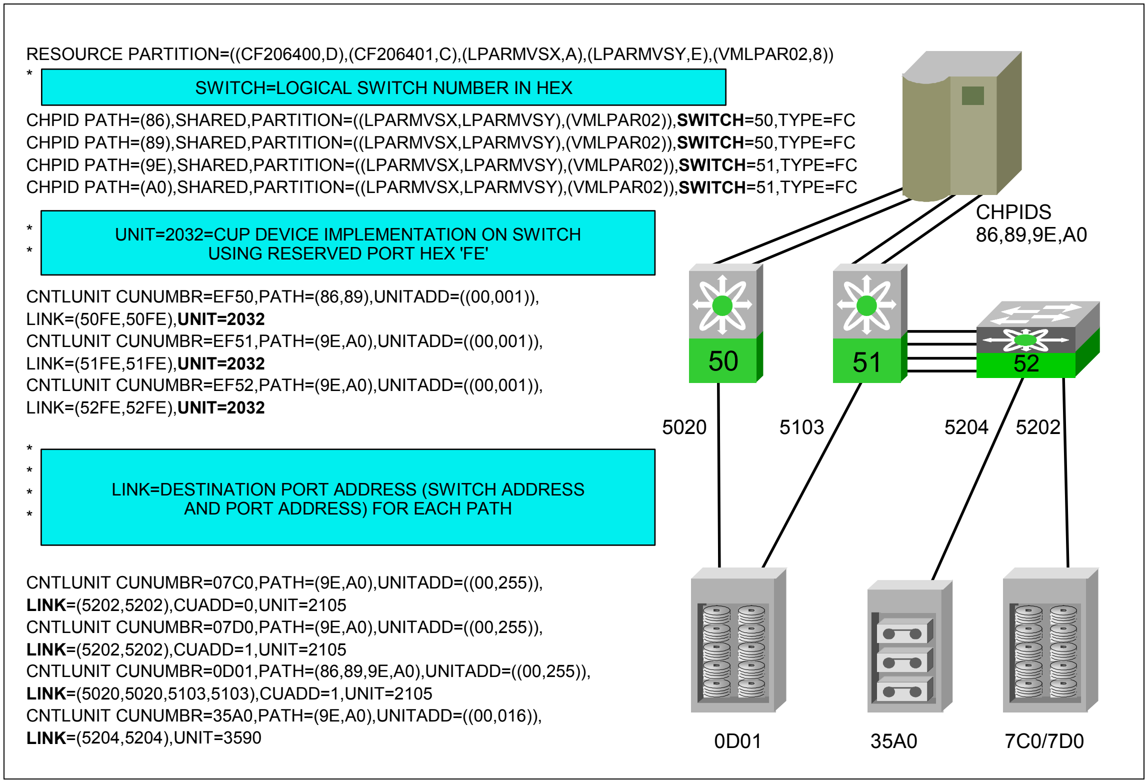
You select your I/O configuration when you:

- POR
- IPL
- Activate a dynamic configuration change

IPL and activation require that you identify the IODF that contains the definition of your configuration. A data set called an I/O configuration data set (IOCDS) is used at POR. An IOCDS can be created from a configuration definition in an IODF. The IOCDS contains the configuration for a specific processor, while the IODF contains configuration data for multiple processors.

Important: We highly recommend that you complete the FICON configuration on the switches before attempting to bring any CHPIDs or Control Units online. The switch configuration cannot be finished until the HCD configuration is complete.

We show an example topology and associated statements in Figure 4-144.



```
RESOURCE PARTITION=((CF206400,D),(CF206401,C),(LPARMVSX,A),(LPARMVSY,E),(VMLPAR02,8))
*           SWITCH=LOGICAL SWITCH NUMBER IN HEX
CHPID PATH=(86),SHARED,PARTITION=((LPARMVSX,LPARMVSY),(VMLPAR02)),SWITCH=50,TYPE=FC
CHPID PATH=(89),SHARED,PARTITION=((LPARMVSX,LPARMVSY),(VMLPAR02)),SWITCH=50,TYPE=FC
CHPID PATH=(9E),SHARED,PARTITION=((LPARMVSX,LPARMVSY),(VMLPAR02)),SWITCH=51,TYPE=FC
CHPID PATH=(A0),SHARED,PARTITION=((LPARMVSX,LPARMVSY),(VMLPAR02)),SWITCH=51,TYPE=FC
*       UNIT=2032=CUP DEVICE IMPLEMENTATION ON SWITCH
*            USING RESERVED PORT HEX 'FE'
CNTLUNIT CUNUMBR=EF50,PATH=(86,89),UNITADD=((00,001)),
LINK=(50FE,50FE),UNIT=2032
CNTLUNIT CUNUMBR=EF51,PATH=(9E,A0),UNITADD=((00,001)),
LINK=(51FE,51FE),UNIT=2032
CNTLUNIT CUNUMBR=EF52,PATH=(9E,A0),UNITADD=((00,001)),
LINK=(52FE,52FE),UNIT=2032
*
*
*   LINK=DESTINATION PORT ADDRESS (SWITCH ADDRESS
*          AND PORT ADDRESS) FOR EACH PATH
CNTLUNIT CUNUMBR=07C0,PATH=(9E,A0),UNITADD=((00,255)),
LINK=(5202,5202),CUADD=0,UNIT=2105
CNTLUNIT CUNUMBR=07D0,PATH=(9E,A0),UNITADD=((00,255)),
LINK=(5202,5202),CUADD=1,UNIT=2105
CNTLUNIT CUNUMBR=0D01,PATH=(86,89,9E,A0),UNITADD=((00,255)),
LINK=(5020,5020,5103,5103),CUADD=1,UNIT=2105
CNTLUNIT CUNUMBR=35A0,PATH=(9E,A0),UNITADD=((00,016)),
LINK=(5204,5204),UNIT=3590
```

Figure 4-144 FICON environment IOCP definitions

> **Note:** There is no change to the IODEVICE or ID statements to support SAN.

We do not propose to cover the HCD definition process, because the reader must be familiar with that before attempting to code any of the statements shown in Figure 4-144.

4.10.1 FICON cascading

The Cisco MDS SAN-OS software allows multiple switches in a FICON network. To configure multiple switches, you must enable and configure fabric binding in each switch. We show how to accomplish this in later sections.

4.11 FICON port numbering on the MDS switches

Default FICON port numbers are assigned by the Cisco MDS SAN-OS software based on the module and the slot in the chassis. The first port in a switch always starts with a zero (0) as shown in Figure 4-145.

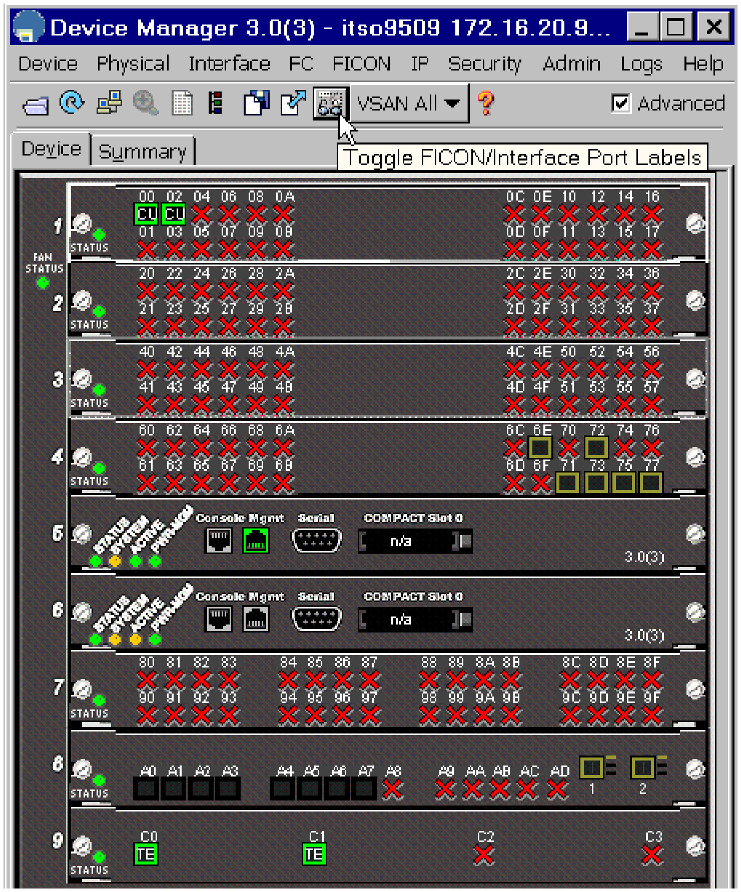

Device Manager 3.0(3) - itso9509 172.16.20.9...
Device Physical Interface FC FICON IP Security Admin Logs Help
VSAN All
☑ Advanced
Device
Summary
Toggle FICON/Interface Port Labels
FAN STATUS
STATUS
1
00 02 04 06 08 0A 0C 0E 10 12 14 16
CU CU
01 03 05 07 09 0B 0D 0F 11 13 15 17
2
20 22 24 26 28 2A 2C 2E 30 32 34 36
21 23 25 27 29 2B 2D 2F 31 33 35 37
3
40 42 44 46 48 4A 4C 4E 50 52 54 56
41 43 45 47 49 4B 4D 4F 51 53 55 57
4
60 62 64 66 68 6A 6C 6E 70 72 74 76
61 63 65 67 69 6B 6D 6F 71 73 75 77
5
STATUS SYSTEM ACTIVE PWR MGMT
Console Mgmt Serial COMPACT Slot 0
n/a
3.0(3)
6
STATUS SYSTEM ACTIVE PWR MGMT
Console Mgmt Serial COMPACT Slot 0
n/a
3.0(3)
7
80 81 82 83 84 85 86 87 88 89 8A 8B 8C 8D 8E 8F
90 91 92 93 94 95 96 97 98 99 9A 9B 9C 9D 9E 9F
8
A0 A1 A2 A3 A4 A5 A6 A7 A8 A9 AA AB AC AD
1 2
9
C0 C1 C2 C3
TE TE

Figure 4-145 Toggle FICON port numbers in Device Manager

The default FICON port number is assigned based on the front panel location of the port and is specific to the slot in which the module resides. Thirty-two (32) port numbers are assigned to each slot on all Cisco MDS 9000 Family switches except for the Cisco MDS 9513 Director, which has 16 port numbers assigned for each slot. These default numbers are assigned regardless of the module's physical presence in the chassis, the port status (up or down), or the number of ports on the module (4, 12, 16, 24, or 48).

If a module has fewer ports than the number of port numbers assigned to the slot, then the excess port numbers are unused. If a module has more ports than the number of port numbers assigned to the slot, the excess ports cannot be used for FICON traffic unless you manually assign the port numbers.

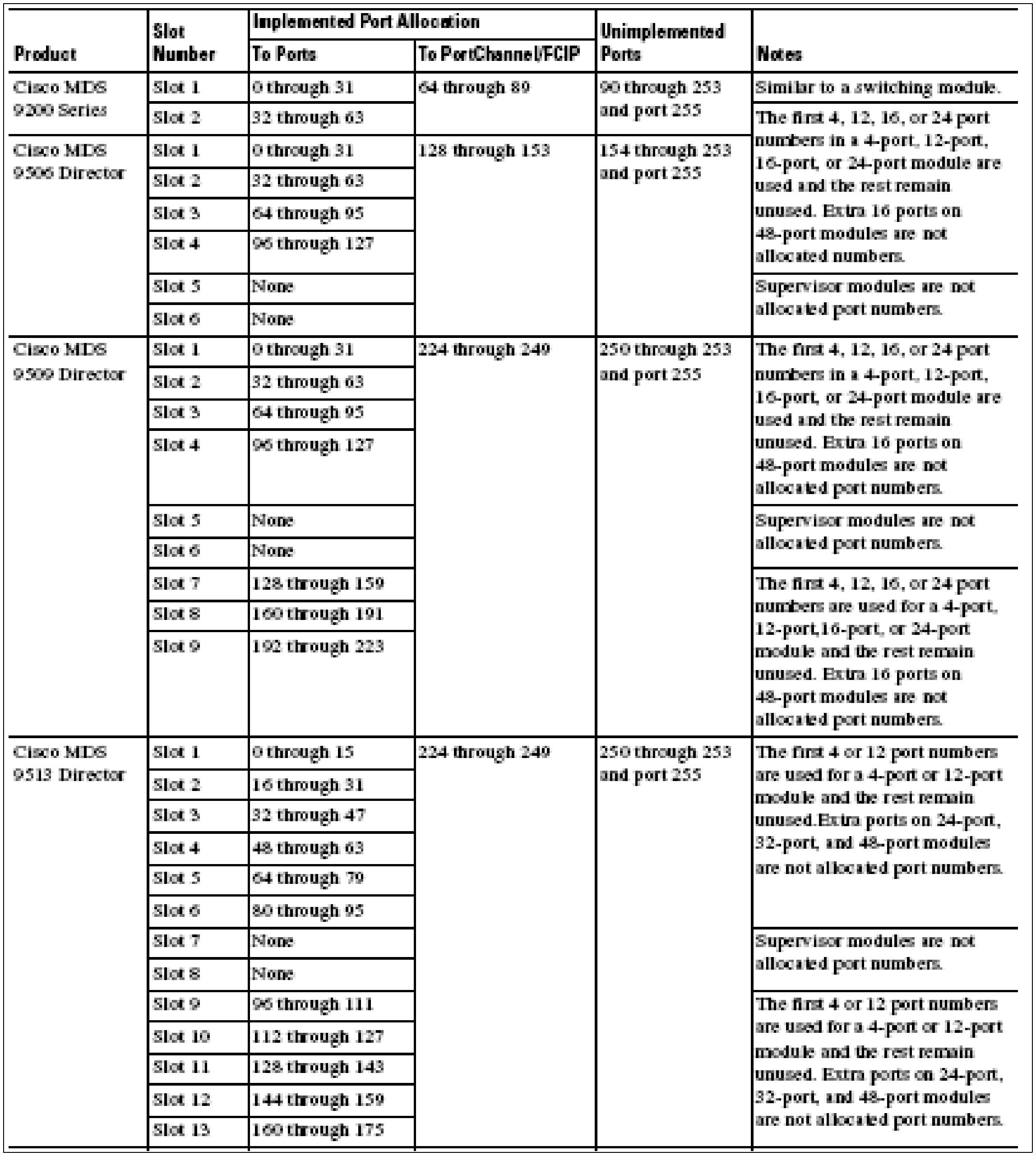
Note: You can set the preference in Device Manager to always display FICON port numbers instead of the default interface numbers by selecting **Device** → **Preferences** → **Label Physical Ports View With**, checking **FICON** and clicking **Apply**.

4.11.1 FICON port number assignment

The FICON port number is assigned based on the front panel location of the port and is specific to the slot in which the module resides. Even if the module is a 16-port module, 32 port numbers are assigned to that module — regardless of the module's physical presence in the chassis or the port status (up or down).

Note: Only Fibre Channel, PortChannel, and FCIP ports are mapped to FICON port numbers. Other types of interfaces do not have a corresponding port number.

Figure 4-146 lists the default port number assignment for the Cisco MDS 9000 Family of switches and directors.



Product	Slot Number	Implemented Port Allocation		Unimplemented Ports	Notes
		To Ports	To PortChannel/FCIP		
Cisco MDS 9200 Series	Slot 1	0 through 31	64 through 89	90 through 253 and port 255	Similar to a switching module.
	Slot 2	32 through 63			The first 4, 12, 16, or 24 port numbers in a 4-port, 12-port, 16-port, or 24-port module are used and the rest remain unused. Extra 16 ports on 48-port modules are not allocated numbers.
Cisco MDS 9506 Director	Slot 1	0 through 31	128 through 153	154 through 253 and port 255	
	Slot 2	32 through 63			
	Slot 3	64 through 95			
	Slot 4	96 through 127			
	Slot 5	None			Supervisor modules are not allocated port numbers.
	Slot 6	None			
Cisco MDS 9509 Director	Slot 1	0 through 31	224 through 249	250 through 253 and port 255	The first 4, 12, 16, or 24 port numbers in a 4-port, 12-port, 16-port, or 24-port module are used and the rest remain unused. Extra 16 ports on 48-port modules are not allocated port numbers.
	Slot 2	32 through 63			
	Slot 3	64 through 95			
	Slot 4	96 through 127			
	Slot 5	None			Supervisor modules are not allocated port numbers.
	Slot 6	None			
	Slot 7	128 through 159			The first 4, 12, 16, or 24 port numbers are used for a 4-port, 12-port,16-port, or 24-port module and the rest remain unused. Extra 16 ports on 48-port modules are not allocated port numbers.
	Slot 8	160 through 191			
	Slot 9	192 through 223			
Cisco MDS 9513 Director	Slot 1	0 through 15	224 through 249	250 through 253 and port 255	The first 4 or 12 port numbers are used for a 4-port or 12-port module and the rest remain unused.Extra ports on 24-port, 32-port, and 48-port modules are not allocated port numbers.
	Slot 2	16 through 31			
	Slot 3	32 through 47			
	Slot 4	48 through 63			
	Slot 5	64 through 79			
	Slot 6	80 through 95			
	Slot 7	None			Supervisor modules are not allocated port numbers.
	Slot 8	None			
	Slot 9	96 through 111			The first 4 or 12 port numbers are used for a 4-port or 12-port module and the rest remain unused. Extra ports on 24-port, 32-port, and 48-port modules are not allocated port numbers.
	Slot 10	112 through 127			
	Slot 11	128 through 143			
	Slot 12	144 through 159			
	Slot 13	160 through 175			

Figure 4-146 Default FICON port numbering

4.11.2 FC ID allocation

FICON requires a predictable and static FC ID allocation scheme. When FICON is enabled, the FC ID allocated to a device is based on the port address of the port to which it is attached. The port address forms the middle byte of the fabric address. Additionally, the last byte of the fabric address should be the same for all devices in the fabric. By default, the last byte value is 0 and can be configured

FCIDs are 3 bytes in length. The first byte is the static domain ID of the switch, in hexadecimal, which matches the switch parameter on the CHPID macro in the IOCDS. The second byte of the FCID is the switch FICON port number port address). The last byte of the FCID defaults to 0. FICON requires the last byte of the fabric address to be the same for all allocated FCIDs. The value of the last byte can be changed if required, but only when the FICON VSAN is in the offline state.

Note: You cannot configure persistent FC IDs in FICON-enabled VSANs.

Cisco MDS switches have a dynamic FC ID allocation scheme. When FICON is enabled or disabled on a VSAN, all the ports are flagged to switch from dynamic to static FC IDs and vice versa. Figure 4-147 shows the static FC ID allocation for FICON.

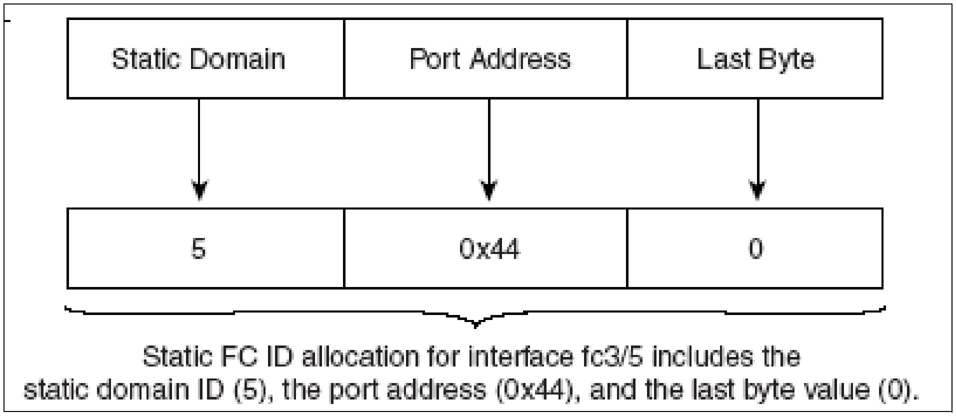

Static Domain
Port Address
Last Byte
5
0x44
0
Static FC ID allocation for interface fc3/5 includes the static domain ID (5), the port address (0x44), and the last byte value (0).

Figure 4-147 Static FC ID allocation

4.11.3 Port addresses

By default, port numbers are the same as port addresses. You can swap the port addresses. We show how to accomplish this in 4.20.2, “Using DM to swap ports” on page 939.

4.11.4 Implemented and unimplemented port addresses

An implemented port refers to any port address that is available in the chassis. An unimplemented port refers to any port address that is not available in the chassis. Refer to Figure 4-146 on page 883.

4.11.5 Reserved FICON port numbering scheme

A range of 255 port numbers are available for you to assign to all the ports on a switch. Figure 4-146 on page 883 shows that you can have more than 255 physical ports on a switch and the excess ports do not have port numbers in the default numbering scheme. When you have more than 255 physical ports on your switch, you can assign unimplemented port numbers to the ports, or assign duplicate port numbers if they are not used in the same FICON VSAN. For example, you can configure port number 1 on interface fc1/1 in FICON VSAN 10 and fc10/1 in FICON VSAN 20.

Note: A FICON VSAN can have a maximum of 250 port numbers.

FICON port numbers are not changed for ports that are active. You must first disable the interfaces using the shutdown command.

You can configure port numbers even when no module is installed in the slot.

4.11.6 Installed and uninstalled ports

An installed port refers to a port for which all required hardware is present. A specified port number in a VSAN can be implemented, and yet not installed, if any of the following conditions apply:

- The module is not present — for example, if module 1 is not physically present in slot 1 in a Cisco MDS 9509 Director, ports 0 to 31 are considered uninstalled.
- The small form-factor pluggable (SFP) port is not present — for example, if a 16-port module is inserted in slot 2 in a Cisco MDS 9509 Director, ports 48 to 63 are considered uninstalled.
- The port is not in a FICON-enabled VSAN — for example, if port 4 (of a 16-port module in slot 1)is configured in FICON-enabled VSAN 2, then only port 4 is installed and ports 0 to 3 and 5 to 15 are uninstalled — even if they are implemented in VSAN 2.
- Another scenario is if VSANs 1 through 5 are FICON-enabled, and trunking-enabled interface fc1/1 has VSANs 3 through 10, then port address 0 is uninstalled in VSAN 1 and 2.

- The port is part of a PortChannel — for example, if interface fc 1/1 is part of PortChanne1 5, port address 0 is uninstalled in all FICON VSANs.

4.11.7 FICON port numbering guidelines

The following guidelines apply to FICON port numbers:

- Supervisor modules do not have port number assignments.
- Port numbers are VSAN independent and do not change based on VSANs or TE ports.
- Each PortChannel must be explicitly associated with a FICON port number.
- When the port number for a physical PortChannel becomes uninstalled, the relevant PortChannel configuration is applied to the physical port.
- Each FCIP tunnel must be explicitly associated with a FICON port number. If the port numbers are not assigned for PortChannels or for FCIP tunnels, the associated ports will not come up.

4.11.8 Assigning FICON port numbers to slots

To assign FICON port numbers to slots using Device Manager, proceed as follows:

Click **FICON** and then select **Port Numbers**. You see the FICON port numbers as shown in Figure 4-148.

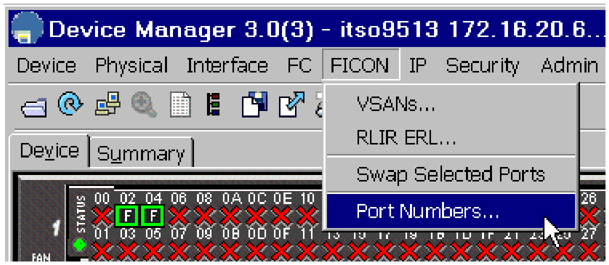
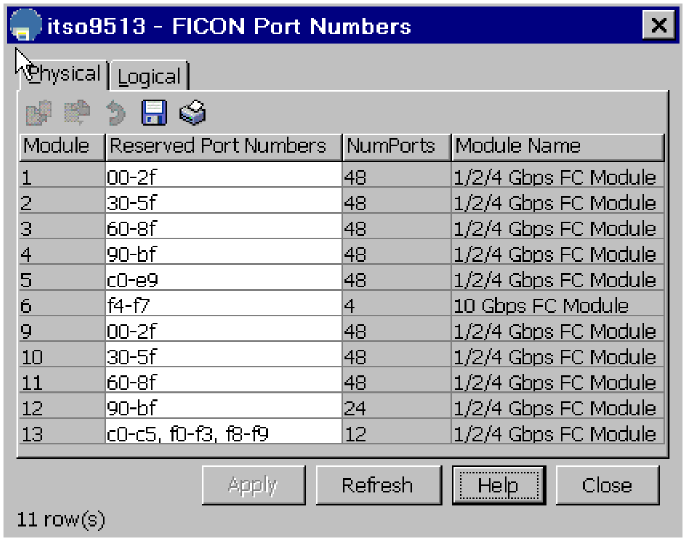

Device Manager 3.0(3) - itso9513 172.16.20.6..
Device
Physical
Interface
FC
FICON
IP
Security
Admin
VSANs...
RLIR ERL...
Swap Selected Ports
Port Numbers...
Device
Summary

Figure 4-148 FICON port numbers

Enter the chassis slot port numbers in the Reserved Port Numbers field (if so desired), click **Apply**, then click **Close**. This panel is shown in Figure 4-149.



Module	Reserved Port Numbers	NumPorts	Module Name
1	00-2f	48	1/2/4 Gbps FC Module
2	30-5f	48	1/2/4 Gbps FC Module
3	60-8f	48	1/2/4 Gbps FC Module
4	90-bf	48	1/2/4 Gbps FC Module
5	c0-e9	48	1/2/4 Gbps FC Module
6	f4-f7	4	10 Gbps FC Module
9	00-2f	48	1/2/4 Gbps FC Module
10	30-5f	48	1/2/4 Gbps FC Module
11	60-8f	48	1/2/4 Gbps FC Module
12	90-bf	24	1/2/4 Gbps FC Module
13	c0-c5, f0-f3, f8-f9	12	1/2/4 Gbps FC Module

11 row(s)

Figure 4-149 Reserving FICON port numbers

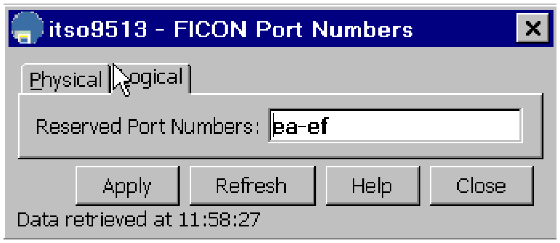
4.11.9 Port numbers for FCIP and PortChannel interfaces

FCIP and PortChannels cannot be used in a FICON-enabled VSAN unless they are explicitly bound to a port number. You can use the default port numbers if they are available or if you reserve port numbers from the pool of port numbers that are not reserved for Fibre Channel interfaces.

Reserving FICON port numbers for FCIP and PortChannel

You must reserve port numbers for logical interfaces, such as FCIP and PortChannels, if you plan to use them. To reserve FICON port numbers for FCIP and PortChannel interfaces using Device Manager, proceed as follows:

Click **FICON** → **Port Numbers**. You see the FICON port numbers as shown in Figure 4-150. Click the **Logical** tab to see the reserved port numbers for the slot.



Reserved Port Numbers: ea-ef

Data retrieved at 11:58:27

Figure 4-150 Reserving port numbers

Enter the chassis slot port numbers. These are the reserved port numbers for one chassis slot. There can be up to 64 port numbers reserved for each slot in the chassis. When you have selected the ports to reserve, click **Apply**, and then click **Close** to complete the operation.

4.12 Cisco MDS 9000 Mainframe Package license

In order to configure the FICON feature on the Cisco MDS switches, the Cisco MDS 9000 Mainframe Package license must be installed first. This license contains the following features:

- FICON protocol and CUP management
- FICON VSAN and intermixing
- Switch cascading
- Fabric binding

Attention: Grace period — the amount of time an application can continue functioning without a license. The grace period is set to 120 days from the first occurrence of using any licensed feature without a license. The grace period starts with the first checkout, and is counted only for the days when that feature is used. If you do not use this feature, the grace period stops incrementing.

To obtain new or updated license key files, follow these steps:

1. Collect the host ID of the switch, also referred to as the switch serial number.
2. Obtain your Claim Certificate or the Proof of Purchase document.
3. Locate the Product Authorization Key (PAK) from the Claim Certificate or Proof of Purchase document.
4. Locate the Web site URL from the Claim Certificate or Proof of Purchase document.

5. Access the specified URL that applies to your switch and enter the switch serial number and the PAK.

The license key file is sent to you by e-mail. The license key file is digitally signed to only authorize use on the switch for which it was requested. The requested features are also enabled once the SAN-OS software on the specified switch access the license key file.

The switch serial number can be seen by obtained by selecting **Physical** → **Inventory** from the Device Manager Tool Bar as illustrated in Figure 4-151.

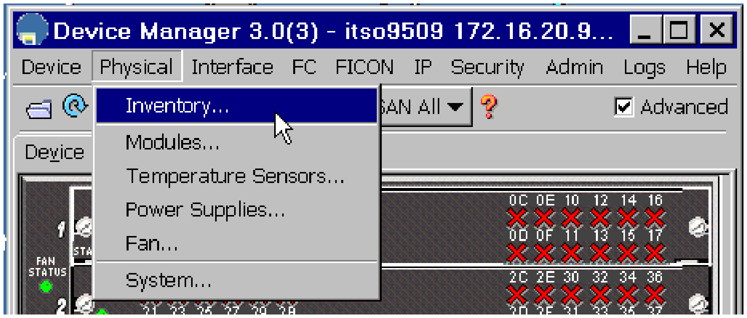
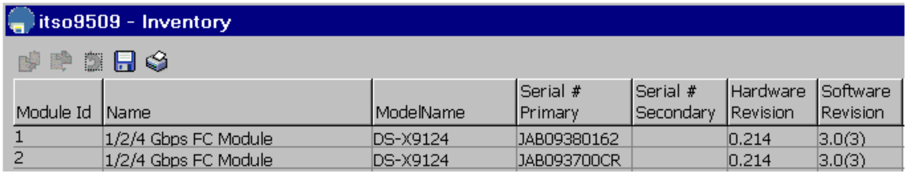

Device Manager 3.0(3) - itso9509 172.16.20.9...
Device
Physical
Interface
FC
FICON
IP
Security
Admin
Logs
Help
Inventory...
Modules...
Temperature Sensors...
Power Supplies...
Fan...
System...
SAN All
Advanced
Device
FAN STATUS

Figure 4-151 Identifying the switch serial number

This displays the model, serial number, and chassis hardware revision level information as shown in Figure 4-152.



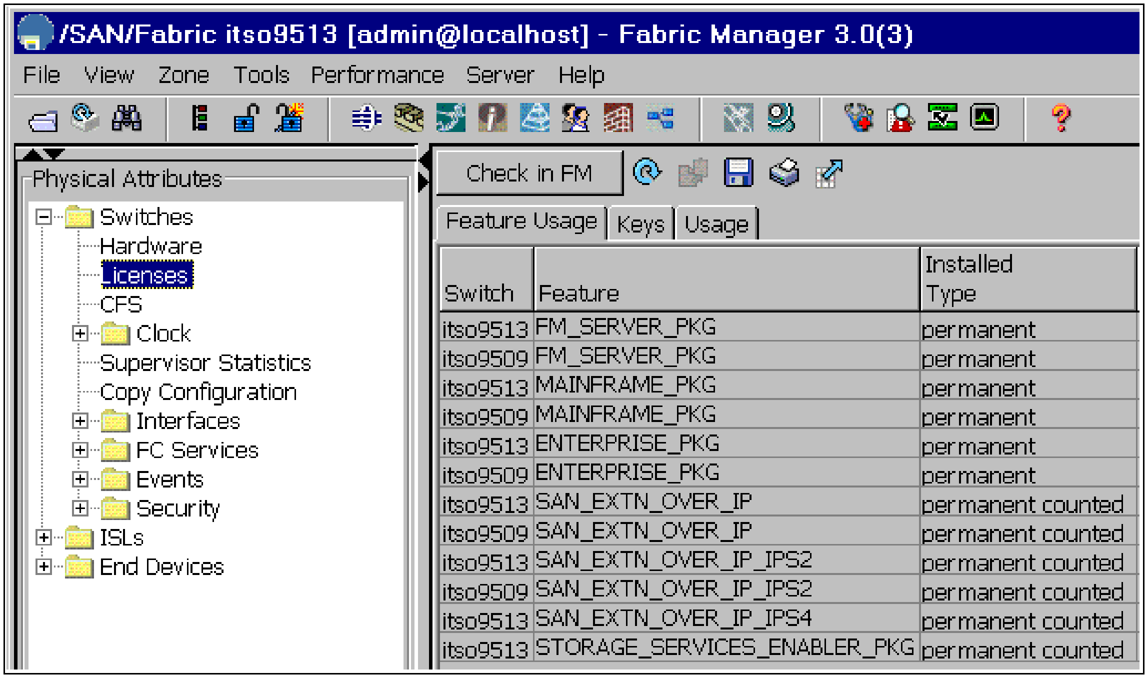
itso9509 - Inventory

Module Id	Name	ModelName	Serial # Primary	Serial # Secondary	Hardware Revision	Software Revision
1	1/2/4 Gbps FC Module	DS-X9124	JAB09380162		0.214	3.0(3)
2	1/2/4 Gbps FC Module	DS-X9124	JAB093700CR		0.214	3.0(3)

Figure 4-152 Switch serial number

When you have received your digitally signed license keys, they can now be installed on the switch. The license files can be copied to the switch bootflash beforehand, or they can be copied during the install process.

You can also use the **Licenses** display in FM to verify that the mainframe licenses have been installed. Open **Licenses** by selecting the **Physical attributes** tab in FM, open the **Switches** folder, and select **Licenses**. In Figure 4-153 we can see the licenses installed.


/SAN/Fabric itso9513 [admin@localhost] - Fabric Manager 3.0(3)
File
View
Zone
Tools
Performance
Server
Help
Physical Attributes
Switches
Hardware
Licenses
CFS
Clock
Supervisor Statistics
Copy Configuration
Interfaces
FC Services
Events
Security
ISLs
End Devices
Check in FM
Feature Usage
Keys
Usage

Switch	Feature	Installed Type
itso9513	FM_SERVER_PKG	permanent
itso9509	FM_SERVER_PKG	permanent
itso9513	MAINFRAME_PKG	permanent
itso9509	MAINFRAME_PKG	permanent
itso9513	ENTERPRISE_PKG	permanent
itso9509	ENTERPRISE_PKG	permanent
itso9513	SAN_EXTN_OVER_IP	permanent counted
itso9509	SAN_EXTN_OVER_IP	permanent counted
itso9513	SAN_EXTN_OVER_IP_IPS2	permanent counted
itso9509	SAN_EXTN_OVER_IP_IPS2	permanent counted
itso9513	SAN_EXTN_OVER_IP_IPS4	permanent counted
itso9513	STORAGE_SERVICES_ENABLER_PKG	permanent counted

Figure 4-153 License verification panel

4.13 FICON VSAN configuration and requirements

One of the advantages of using the Cisco MDS switches in mixed FCP (open systems) and FICON environments is the ability to separate FICON and FCP traffic into separate VSANs. This is considered best practice. The capability exists, if desired, to mix FCP and FICON traffic into a single VSAN and use zoning to separate the two, but this is *not* the recommended design.

Using separate VSANs provide the following functionality:

- Better isolation is possible.
- VSAN based roles for administrative access can be created.
- In-order delivery can be set per VSAN.
- Load balancing behavior can be set per VSAN.
- Default zoning behavior can be set per VSAN.
- Persistent FCIDs can be set per VSAN.
- Domain ID allocation (static or dynamic) behavior can be set per VSAN.
- Fibre Channel timers can be set per VSAN.

This is not an all inclusive list; it is an overview of how using the VSAN feature allows you to implement FCP and FICON over the same physical topology without sacrificing specific features as a result of FCP or FICON specific fabric/VSAN requirements.

4.13.1 FICON VSAN prerequisites

To ensure that a FICON VSAN is correctly set up, be sure to verify the following requirements:

- Set the default zone to permit if you are not using the zoning feature.
- Enable in-order delivery on the VSAN.
- Enable (and if required, configure) fabric binding on the VSAN.
- Verify that conflicting persistent FC IDs do not exist in the switch.
- Verify that the configured domain ID and requested domain ID match.
- Add the control unit port (CUP) (area FE) to the zone, if you are using zoning.

If any of these requirements are not met, the FICON feature cannot be enabled.

Next we show the creation of FICON VSAN 2. We again use FM to create the cascaded FICON VSAN (VSAN 2) between the 9509 and 9513. We then repeat the process using FM to create the point-to-point FICON VSAN 3 that will reside on the 9513.

At this point in time we connect the interswitch links between the 9509 and the 9513. This allows us to manage both the 9509 and 9513 switches in the FICON cascaded fabric concurrently.

There are several ways to bring ports online, but perhaps the most intuitive way is to use DM.

In Figure 4-154 we loaded DM for the 9506, and have clicked on interface FC9/2 and FC9/1 by holding the CTRL key to highlight both interfaces. We then right-clicked and selected **Enable** from the pull-down list.

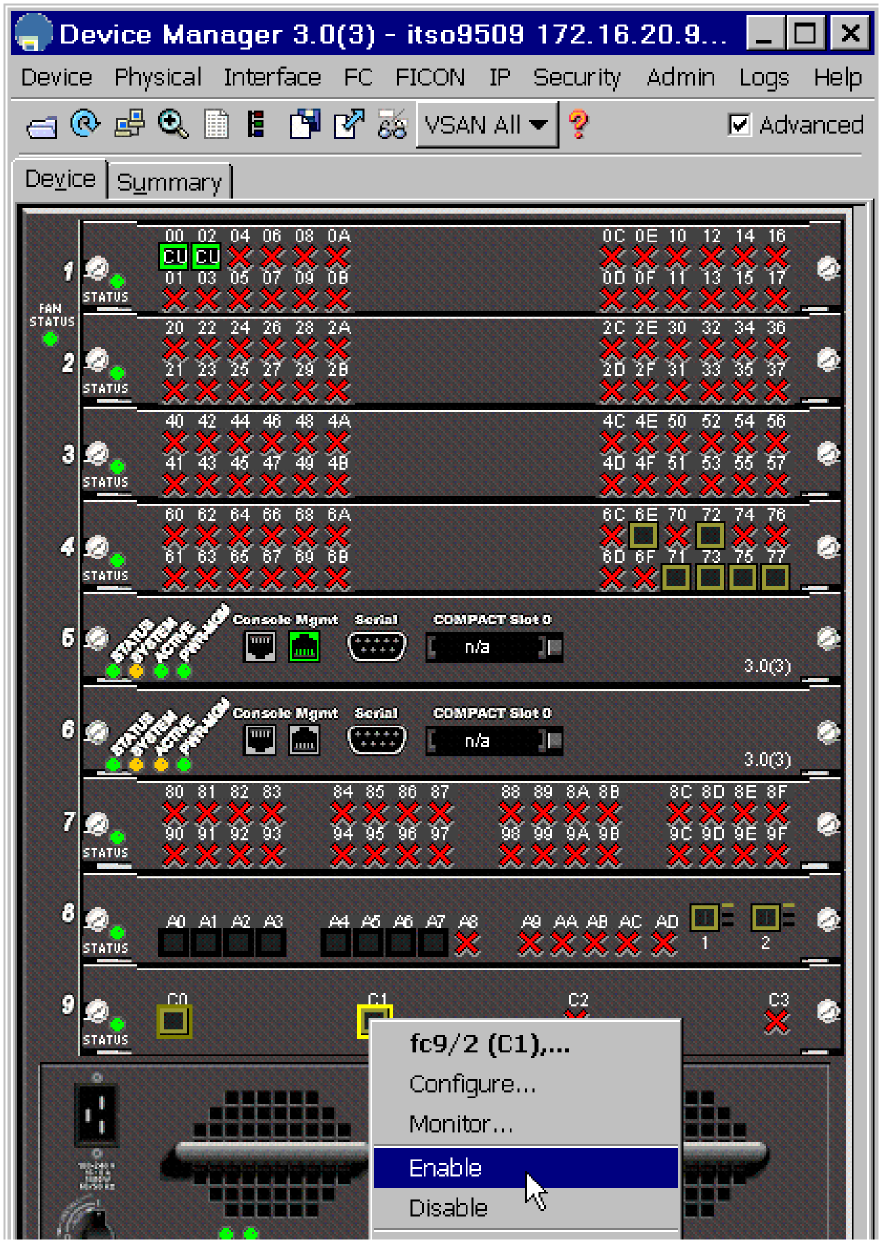

Device Manager 3.0(3) - itso9509 172.16.20.9...
Device
Physical
Interface
FC
FICON
IP
Security
Admin
Logs
Help
VSAN All
Advanced
Device
Summary
FAN STATUS
STATUS
Console Mgmt
Serial
COMPACT Slot 0
n/a
3.0(3)
fc9/2 (C1),...
Configure...
Monitor...
Enable
Disable

Figure 4-154 Enable E_Ports in Device Manager on the 9509

The same must be done in DM for interfaces FC6/1 and FC6/2 on the 9513 as shown in Figure 4-155.

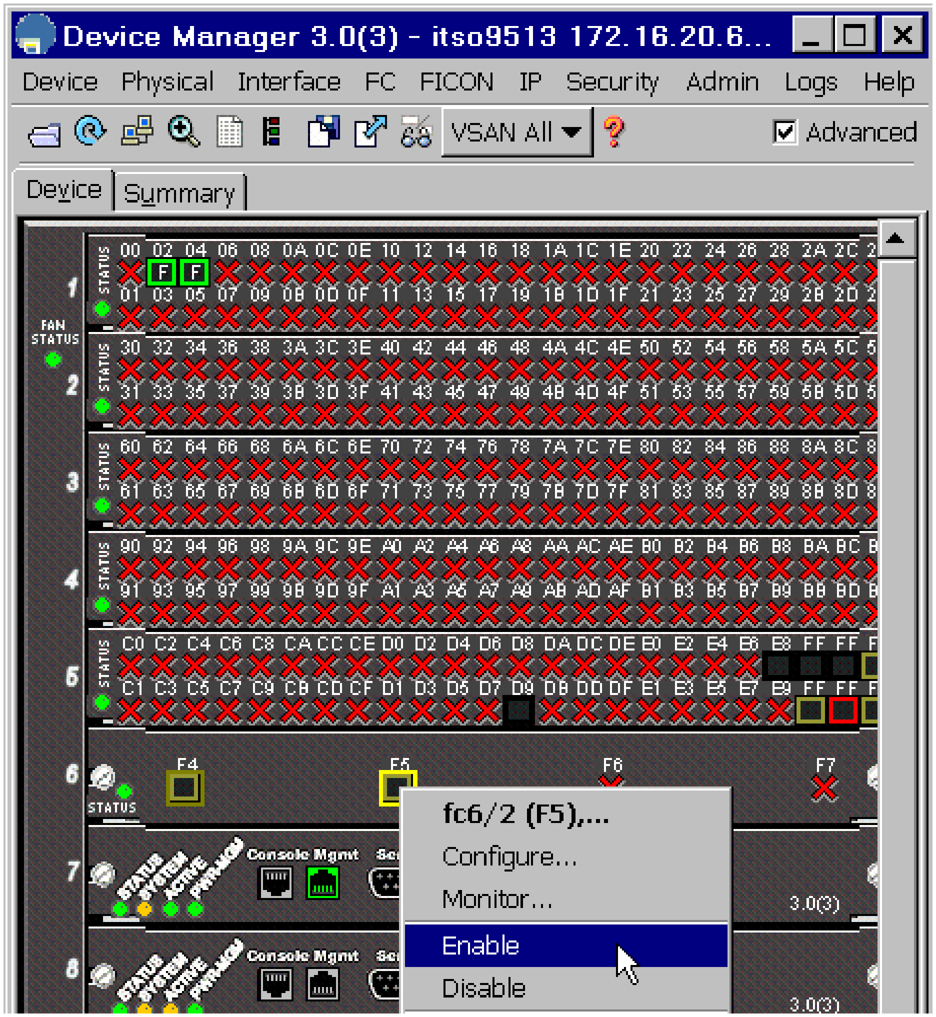

Device Manager 3.0(3) - itso9513 172.16.20.6...
Device Physical Interface FC FICON IP Security Admin Logs Help
VSAN All
☑ Advanced
Device
Summary
F4
F5
F6
F7
fc6/2 (F5),...
Configure...
Monitor...
Enable
Disable

Figure 4-155 Enable E_Ports on 9513

At this point, if we refresh the DM Device view window, in a couple of seconds we see a **TE** indication on the port. This means that the ISLs are up and trunking as shown in Figure 4-156.

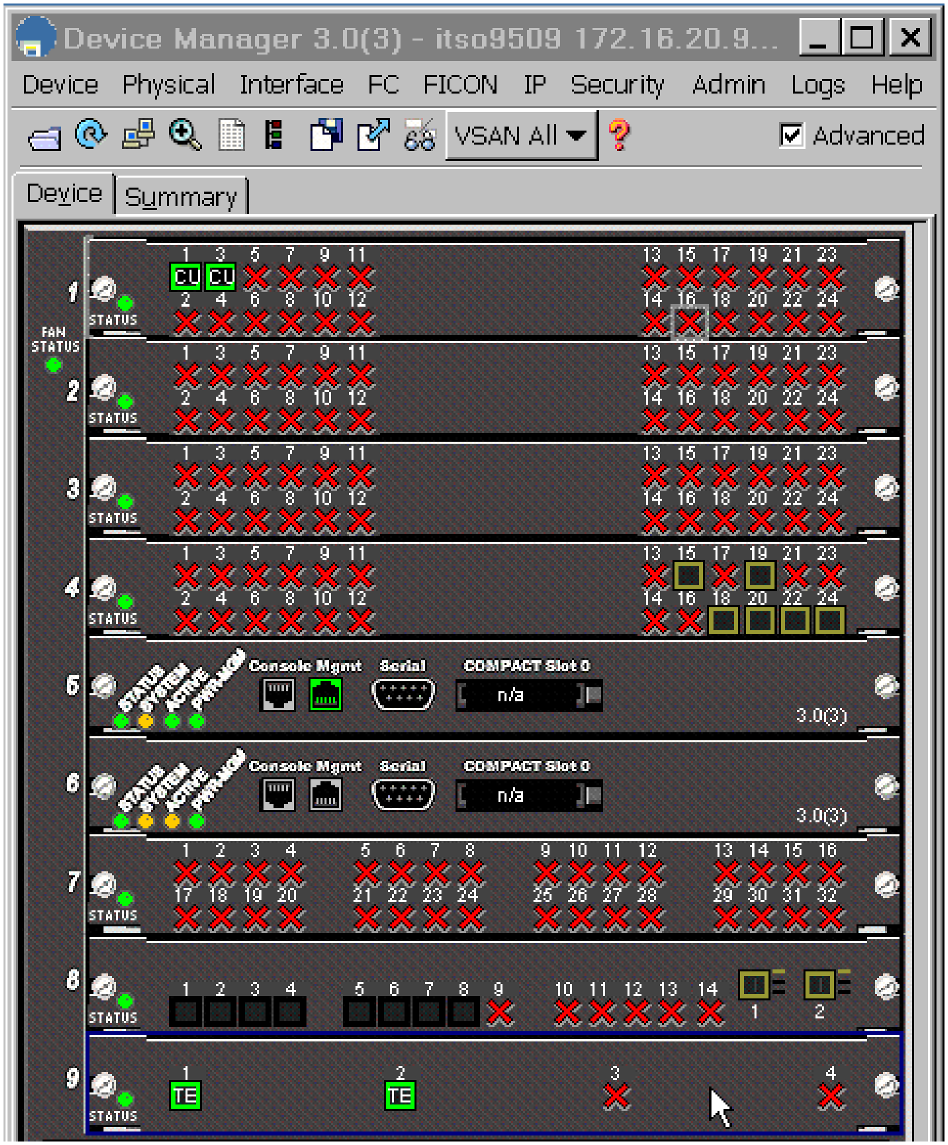
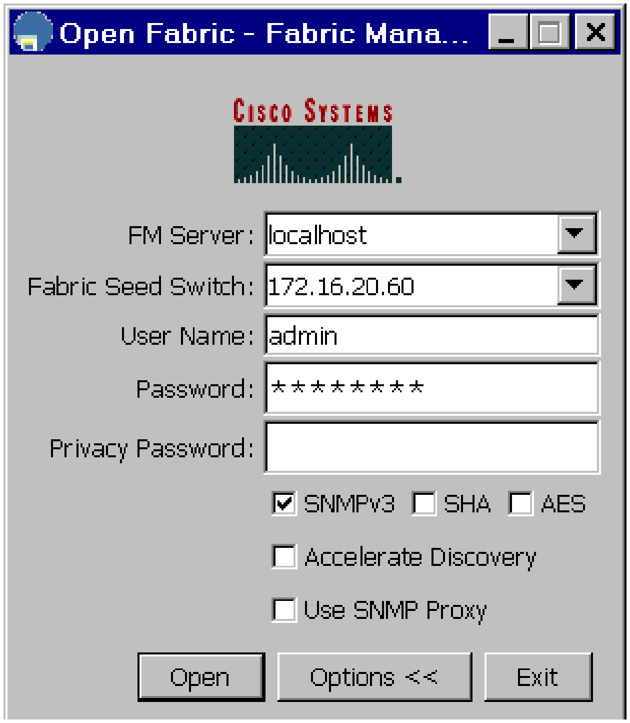

Device Manager 3.0(3) - itso9509 172.16.20.9...
Device
Physical
Interface
FC
FICON
IP
Security
Admin
Logs
Help
VSAN All
☑ Advanced
Device
Summary
FAN STATUS
STATUS
CU
TE
Console Mgmt
Serial
COMPACT Slot 0
n/a
3.0(3)

Figure 4-156 Verify ISL links are up

To begin configuring cascaded FICON VSAN 2, we log in to FM using the FM server located at IP address `172.16.20.60` as shown in Figure 4-157.


Open Fabric - Fabric Mana...
Cisco Systems

FM Server: localhost

Fabric Seed Switch: 172.16.20.60

User Name: admin

Password: ********

Privacy Password:

☑ SNMPv3 ☐ SHA ☐ AES

☐ Accelerate Discovery

☐ Use SNMP Proxy

Open
Options <<
Exit

Figure 4-157 Logging in to FM server

Next, select the **Create VSAN** wizard as indicated in Figure 4-158.

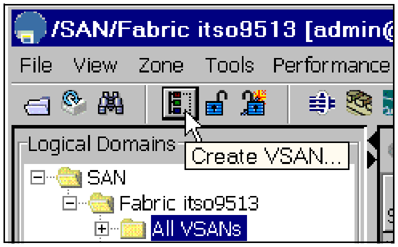
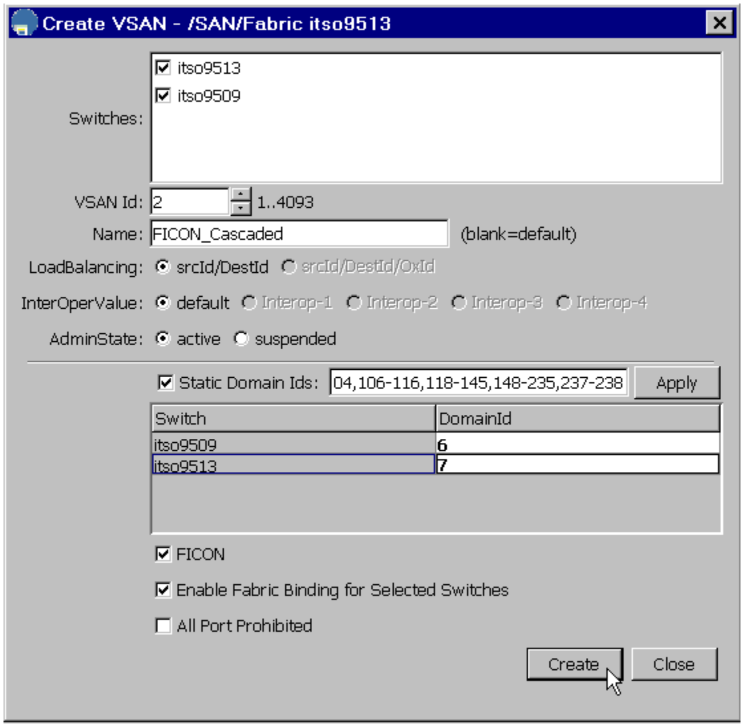

/SAN/Fabric itso9513 [admin@
File View Zone Tools Performance
Logical Domains
Create VSAN...
SAN
Fabric itso9513
All VSANs

Figure 4-158 Create VSAN wizard

This opens another panel as shown in Figure 4-159.

Take note of the following items that are selected in this panel:

- Both itso9509 and itso9513 are selected. VSAN 2 will be created on each switch.
- A VSAN ID of 2 is entered.
- The name FICON_Cascaded is given to this VSAN.
- Source ID / Destination ID is selected (FICON requirement).
- InteropValue is left to default (required).
- Admin state is active.
- The FICON feature is enabled for this VSAN.
- Fabric Binding is enabled for this VSAN (required).
- Static domain ID is selected, assigned, and matches what is configured on the mainframe in HCD.



Create VSAN - /SAN/Fabric itso9513

Switches:
☑ itso9513
☑ itso9509

VSAN Id: 2 1..4093

Name: FICON_Cascaded (blank=default)

LoadBalancing: ● srcId/DestId ○ srcId/DestId/OxId

InterOperValue: ● default ○ Interop-1 ○ Interop-2 ○ Interop-3 ○ Interop-4

AdminState: ● active ○ suspended

☑ Static Domain Ids: 04,106-116,118-145,148-235,237-238 Apply

Switch	DomainId
itso9509	6
itso9513	7

☑ FICON

☑ Enable Fabric Binding for Selected Switches

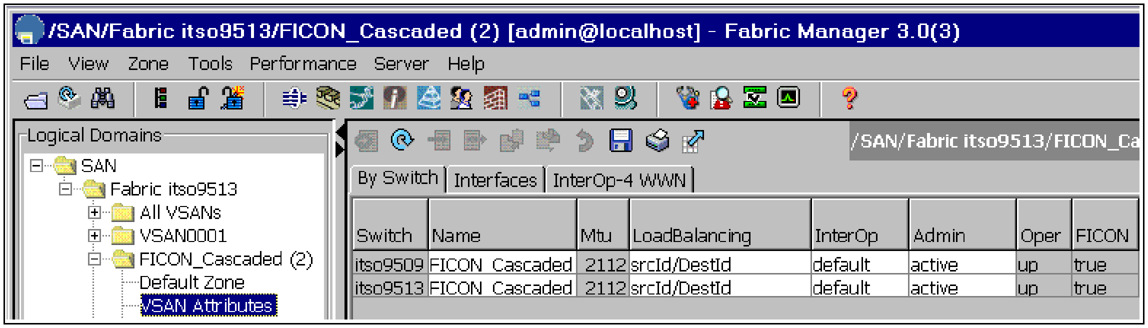
☐ All Port Prohibited

Figure 4-159 VSAN creation panel

When the FICON feature in Cisco MDS switches is enabled, the following operations occur automatically.

- The IPL configuration file is automatically created (as discussed in “FICON configuration files” on page 931).
- The in-order delivery, source-destination id load balancing, fabric binding, and static (insistent) domain ID features are enabled for this VSAN and cannot be disabled.
- The default zoning behavior is changed to permit.

We can verify that FICON VSAN 2 was created on each switch with the correct attributes. We do this by selecting the **Logical Domains** tab in FM, opening the **FICON_Cascaded(2)** folder, and selecting **VSAN Attributes** as shown in Figure 4-160.

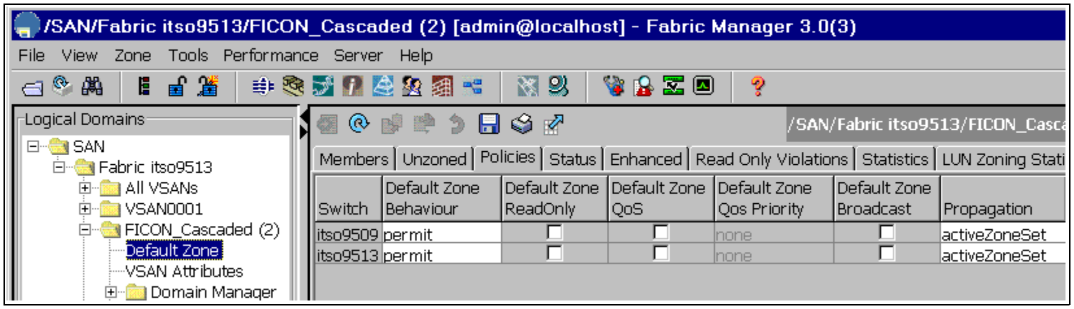

/SAN/Fabric itso9513/FICON_Cascaded (2) [admin@localhost] - Fabric Manager 3.0(3)
File
View
Zone
Tools
Performance
Server
Help
Logical Domains
SAN
Fabric itso9513
All VSANs
VSAN0001
FICON_Cascaded (2)
Default Zone
VSAN Attributes
/SAN/Fabric itso9513/FICON_Ca
By Switch
Interfaces
InterOp-4 WWN

Switch	Name	Mtu	LoadBalancing	InterOp	Admin	Oper	FICON
itso9509	FICON Cascaded	2112	srcId/DestId	default	active	up	true
itso9513	FICON Cascaded	2112	srcId/DestId	default	active	up	true

Figure 4-160 VSAN verification panel one

The default zone behavior (permit is required) can be verified by opening the folder for the VSAN created, **FICON_Cascaded** in this case, selecting **Default Zone**, and then selecting the **Policies** tab as shown in Figure 4-161.

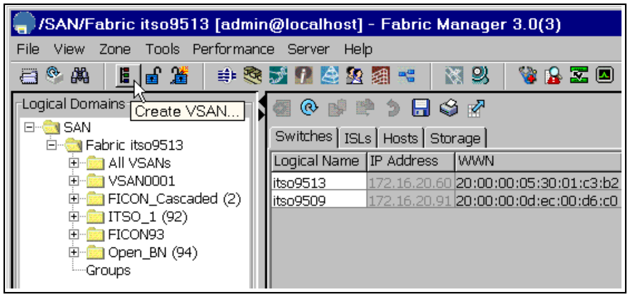
> **Tip:** Using descriptive names for your VSANs helps you to identify them more easily in FM, and leads to less confusion and mistakes.


/SAN/Fabric itso9513/FICON_Cascaded (2) [admin@localhost] - Fabric Manager 3.0(3)
File View Zone Tools Performance Server Help
Logical Domains
SAN
Fabric itso9513
All VSANs
VSAN0001
FICON_Cascaded (2)
Default Zone
VSAN Attributes
Domain Manager
/SAN/Fabric itso9513/FICON_Casca
Members Unzoned Policies Status Enhanced Read Only Violations Statistics LUN Zoning Stati

Switch	Default Zone Behaviour	Default Zone ReadOnly	Default Zone QoS	Default Zone Qos Priority	Default Zone Broadcast	Propagation
itso9509	permit	☐	☐	none	☐	activeZoneSet
itso9513	permit	☐	☐	none	☐	activeZoneSet

Figure 4-161 Default zone policy verification

Now that cascaded FICON VSAN 2 has been created, we proceed with the configuration of point-to-point FICON VSAN 3 on the 9513 using the standalone version of FM. For this we again log into FM. Once again, we select the **Create** VSAN Wizard icon as shown in Figure 4-162.


/SAN/Fabric itso9513 [admin@localhost] - Fabric Manager 3.0(3)
File View Zone Tools Performance Server Help
Logical Domains
Create VSAN...
SAN
Fabric itso9513
All VSANs
VSAN0001
FICON_Cascaded (2)
ITSO_1 (92)
FICON93
Open_BN (94)
Groups
Switches ISLs Hosts Storage

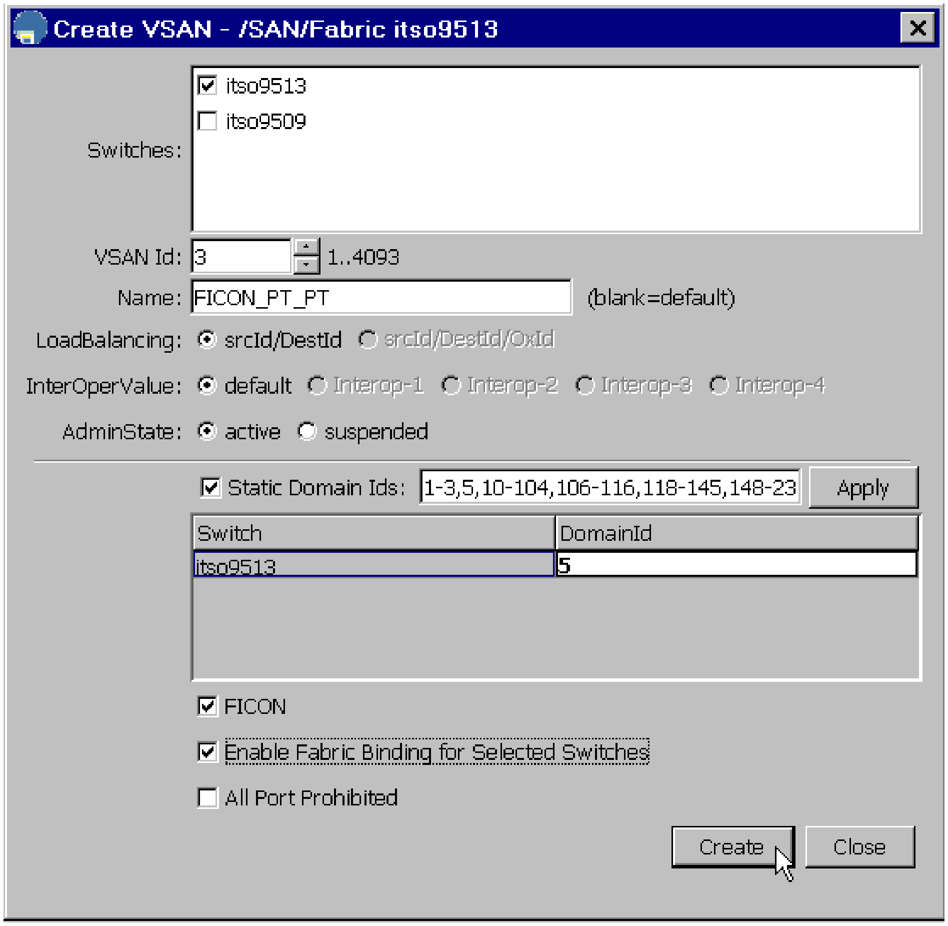
Logical Name	IP Address	WWN
itso9513	172.16.20.60	20:00:00:05:30:01:c3:b2
itso9509	172.16.20.91	20:00:00:0d:ec:00:d6:c0

Figure 4-162 VSAN Create Wizard

This opens the **VSAN Attributes/Create** panel as shown in Figure 4-163.

Take note of the following items that are selected in this panel:

- Only switch itso9513 is selected.
- A VSAN ID of 3 is entered.
- The name FICON_PT_PT is given to this VSAN.
- Source ID / Destination ID is selected (FICON requirement).
- Interop value is left to default (required).
- Admin state is active.
- The FICON feature is enabled for this VSAN.
- Fabric Binding is enabled for this VSAN (required).
- Static domain ID 5 is selected (static domain ID is selected, assigned, and matches what is configured on the mainframe in HCD).


Create VSAN - /SAN/Fabric itso9513

Switches:
☑ itso9513
☐ itso9509

VSAN Id: 3 1..4093

Name: FICON_PT_PT (blank=default)

LoadBalancing: ● srcId/DestId ○ srcId/DestId/OxId

InterOperValue: ● default ○ Interop-1 ○ Interop-2 ○ Interop-3 ○ Interop-4

AdminState: ● active ○ suspended

☑ Static Domain Ids: 1-3,5,10-104,106-116,118-145,148-23

Switch	DomainId
itso9513	5

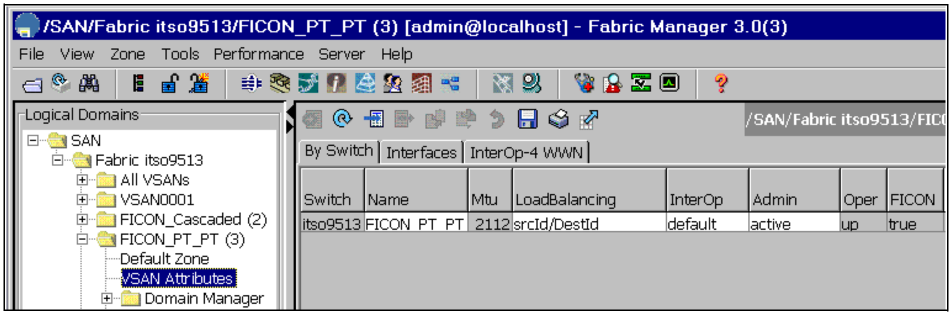
☑ FICON

☑ Enable Fabric Binding for Selected Switches

☐ All Port Prohibited

Figure 4-163 FICON point-to-point VSAN creation

We can verify that FICON VSAN 2 was created on the `9513` with the correct attributes by selecting the **Logical Domains** tab in FM, opening the **FICON_PT_PT** folder, and selecting **VSAN Attributes** as shown in Figure 4-163.

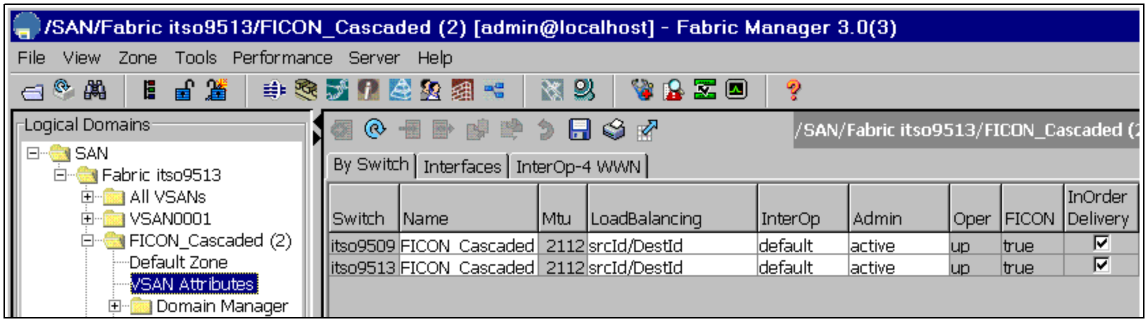

/SAN/Fabric itso9513/FICON_PT_PT (3) [admin@localhost] - Fabric Manager 3.0(3)
File View Zone Tools Performance Server Help
Logical Domains
SAN
Fabric itso9513
All VSANs
VSAN0001
FICON_Cascaded (2)
FICON_PT_PT (3)
Default Zone
VSAN Attributes
Domain Manager
/SAN/Fabric itso9513/FIC
By Switch
Interfaces
InterOp-4 WWN

Switch	Name	Mtu	LoadBalancing	InterOp	Admin	Oper	FICON
itso9513	FICON_PT_PT	2112	srcId/DestId	default	active	up	true

Figure 4-164 FICON point-to-point VSAN verification

The default zone behavior (permit required) can be verified by opening the folder for the VSAN created, **FICON_PT_PT** but in this case by selecting **Default Zone**, and then selecting the **Policies** tab.

The setting for in-order delivery can be verified by opening the desired VSAN folder, **FICON_Cascaded** in this case, selecting **VSAN Attributes**, and then selecting the **By Switch** tab as shown in Figure 4-165.


/SAN/Fabric itso9513/FICON_Cascaded (2) [admin@localhost] - Fabric Manager 3.0(3)
File View Zone Tools Performance Server Help
Logical Domains
SAN
Fabric itso9513
All VSANs
VSAN0001
FICON_Cascaded (2)
Default Zone
VSAN Attributes
Domain Manager
/SAN/Fabric itso9513/FICON_Cascaded (
By Switch
Interfaces
InterOp-4 WWN

Switch	Name	Mtu	LoadBalancing	InterOp	Admin	Oper	FICON	InOrder Delivery
itso9509	FICON_Cascaded	2112	srcId/DestId	default	active	up	true	☑
itso9513	FICON_Cascaded	2112	srcId/DestId	default	active	up	true	☑

Figure 4-165 In-order delivery verification

4.14 FICON load balancing

FICON uses a load balancing algorithm based upon source and destination ID, so some additional planning is necessary when deciding how ISLs, both FC and FCIP, are to be designed. An automated tool in FM has been developed to aid in this exercise. This tool is the **FICON Flow Load Balance Calculator** shown in Figure 4-166.

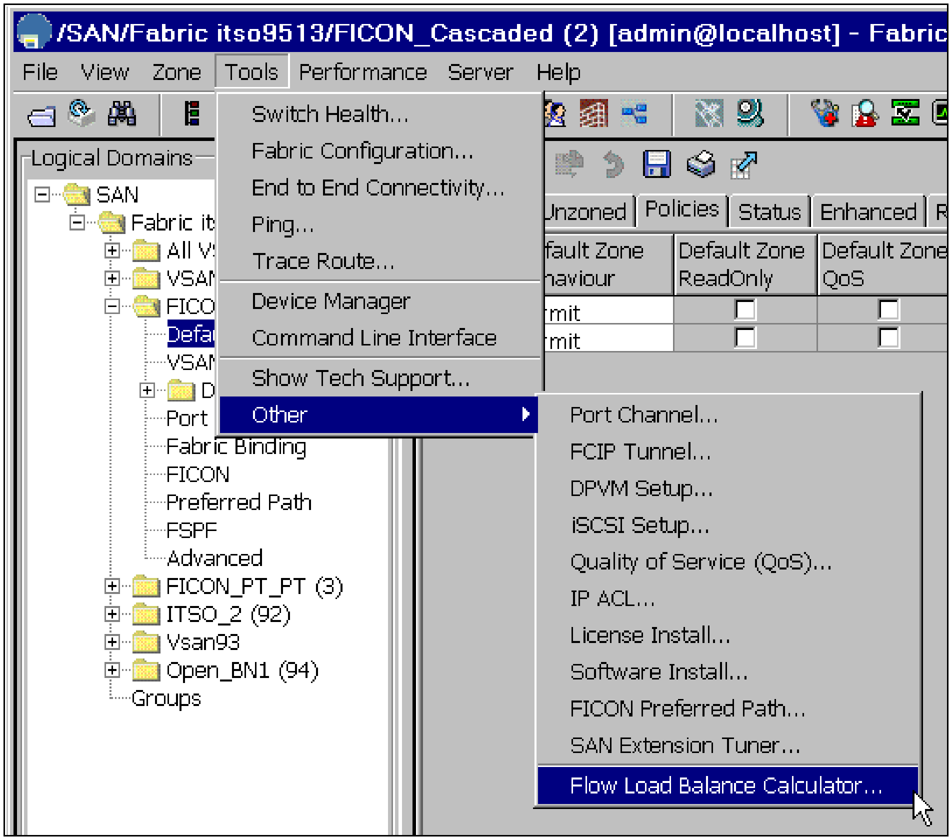
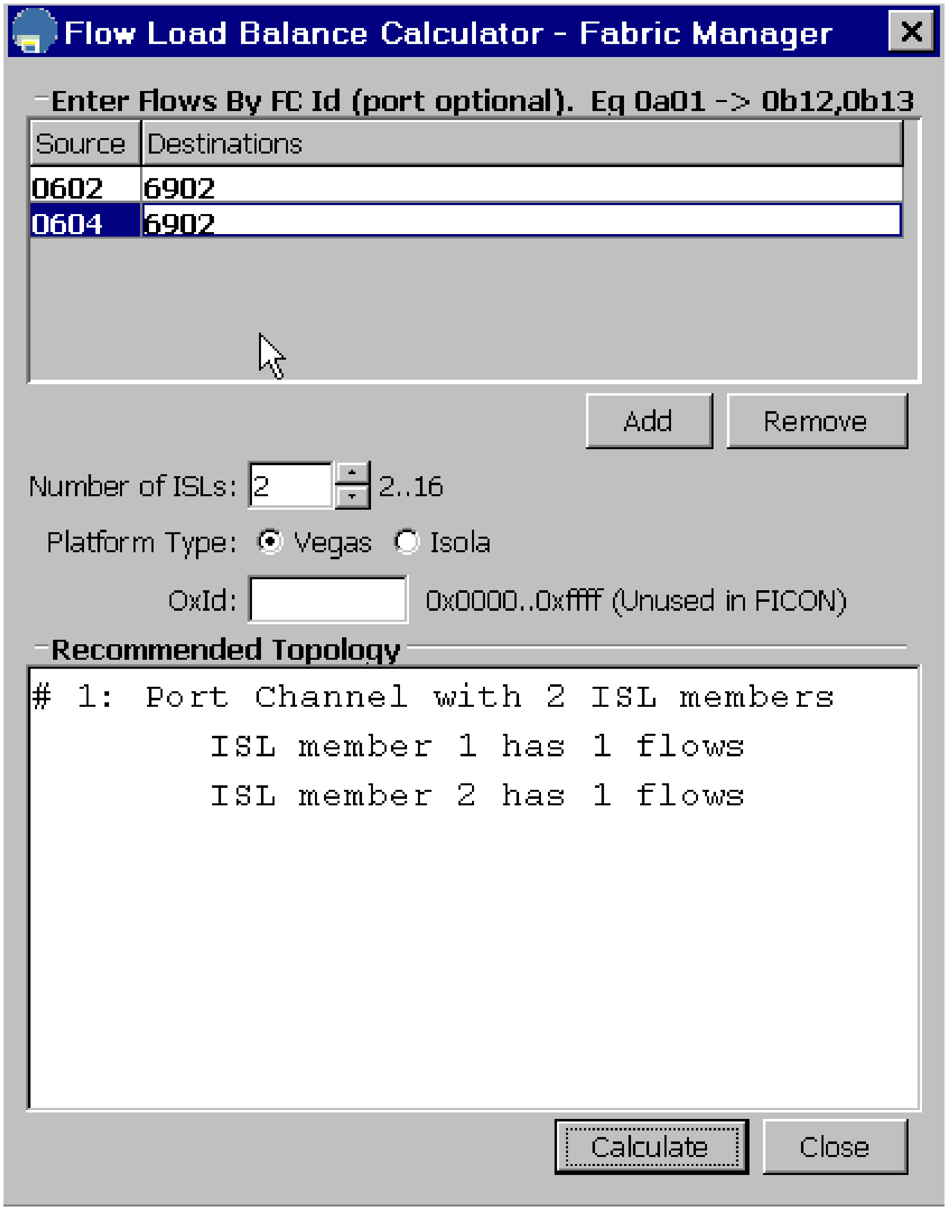

/SAN/Fabric itso9513/FICON_Cascaded (2) [admin@localhost] - Fabric
File View Zone Tools Performance Server Help
Switch Health...
Fabric Configuration...
End to End Connectivity...
Ping...
Trace Route...
Device Manager
Command Line Interface
Show Tech Support...
Other
Port Channel...
FCIP Tunnel...
DPVM Setup...
iSCSI Setup...
Quality of Service (QoS)...
IP ACL...
License Install...
Software Install...
FICON Preferred Path...
SAN Extension Tuner...
Flow Load Balance Calculator...
Logical Domains
SAN
Fabric it
All V
VSAN
FICO
Defa
VSAN
D
Port
Fabric Binding
FICON
Preferred Path
FSPF
Advanced
FICON_PT_PT (3)
ITSO_2 (92)
Vsan93
Open_BN1 (94)
Groups
Unzoned
Policies
Status
Enhanced
fault Zone haviour
Default Zone ReadOnly
Default Zone QoS
mit
mit

Figure 4-166 FM FICON Flow Load Balance Calculator

Figure 4-167 on page 902 shows the calculator. To determine the proper ISL configuration, we clicked the **Add** button twice, entered the **Source** and **Destinations** flows from **Source** (FCIDS 0x**0602**00 and 0x**0604**00) to the **Destinations** (FCID 0x**6902**00).

We then selected that two ISLs would be used (in this case the ISLs were FCIP links), clicked **Calculate**, and the **Recommended Topology** appears as shown in Figure 4-167.


Flow Load Balance Calculator - Fabric Manager
Add
Remove
Calculate
Close

Enter Flows By FC Id (port optional). Eq 0a01 -> 0b12,0b13

Source	Destinations
0602	6902
0604	6902

Number of ISLs: 2 2..16

Platform Type: ● Vegas ○ Isola

OxId: 0x0000..0xffff (Unused in FICON)

Recommended Topology

```
# 1:  Port Channel with 2 ISL members
         ISL member 1 has 1 flows
         ISL member 2 has 1 flows
```

Figure 4-167 FM FICON Flow Load Balance Calculator

Note: Platform Type of Vegas refers to Generation 1 linecards (1 and 2 MBs), whereas Isola refers to Generation 2 linecards (1, 2, and 4 MBs) .

4.15 Static domain ID configuration

As mentioned previously, static (insistent) domain IDs are a requirement for FICON. The use of static domain IDs is required because this information is statically coded in the IOCDS `CHPID` and `CNTLUNIT` macros, and is part of the fabric binding database. MDS switches have a concept of a running and configured domain ID. After you change the domain ID and make it static, you must disruptively restart this VSAN in order for the newly configured domain ID to take effect.

Note: This is automatically done as part of the FM FICON VSAN create wizard.

4.16 Fabric binding configuration

Fabric binding is a security feature that allows us to explicitly control which switches can be part of a fabric by manually defining the authorized switches in a fabric binding database. This prevents non-authorized switches from joining the fabric either accidentally or intentionally. Each FICON switch that is allowed to connect to the fabric must be added to the fabric binding database of every other FICON switch in the fabric. Activating fabric binding is a prerequisite for enabling FICON on a VSAN.

In FICON cascaded topology the fabric binding database contains the switch World Wide Name (sWWN) and domain ID of all the switches authorized to join the fabric. Fabric binding authorization is enforced per VSAN, as each VSAN is a logical fabric. In a FICON point-to-point topology fabric binding is still required but the fabric binding database is empty because defining the local sWWN and domain ID in the fabric binding database is not required.

There are two fabric binding databases:

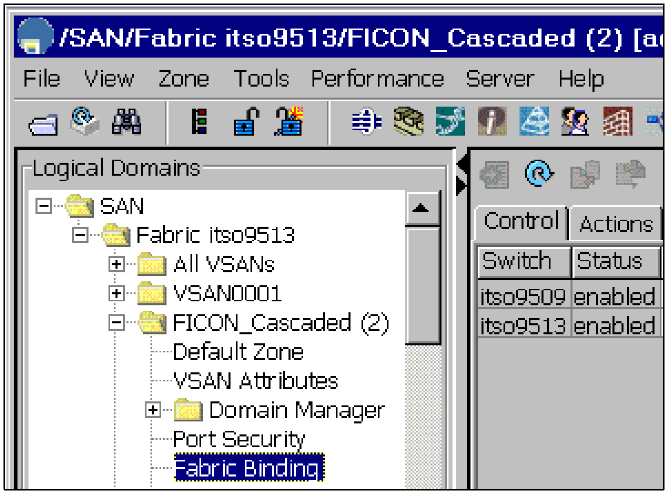
- **Configuration database:** contains all the manually configured SWWNs and domain IDs of those switches that are authorized to join the fabric
- **Active database:** contains the entries that are currently being enforced in the fabric.

In order to start enforcing a newly created or modified configuration database, an activation sequence must be performed. The activation replaces the active database with the configured database. This activation fails if the configured database does not match the current state of the fabric — for example, if a switch is currently in the fabric but not defined in the database, or if a switch is in the fabric but currently has a different domain ID than is defined in the configuration database. Alternatively, the force option could be used to activate the new fabric binding configuration which isolates the switch in question.

Attention: It would be very easy to make a mistake in the configured fabric binding database by using the force option and causing isolation to occur in the fabric. The force option must be used with discretion and care.

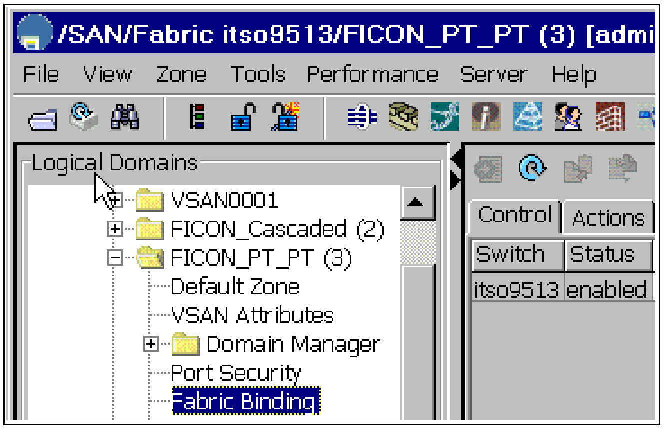
Next, we proceed with the verification of the fabric binding database for both the point-to-point VSAN 3 and the cascaded VSAN 2.

To verify that fabric binding is enabled, we open the folder of the VSAN we want to examine by selecting **Fabric Binding**, and examining the Status column as shown in Figure 4-168 and Figure 4-169.


/SAN/Fabric itso9513/FICON_Cascaded (2) [a
File
View
Zone
Tools
Performance
Server
Help
Logical Domains
SAN
Fabric itso9513
All VSANs
VSAN0001
FICON_Cascaded (2)
Default Zone
VSAN Attributes
Domain Manager
Port Security
Fabric Binding
Control
Actions

Switch	Status
itso9509	enabled
itso9513	enabled

Figure 4-168 Fabric binding status of VSAN 2


/SAN/Fabric itso9513/FICON_PT_PT (3) [admi
File View Zone Tools Performance Server Help
Logical Domains
VSAN0001
FICON_Cascaded (2)
FICON_PT_PT (3)
Default Zone
VSAN Attributes
Domain Manager
Port Security
Fabric Binding
Control
Actions

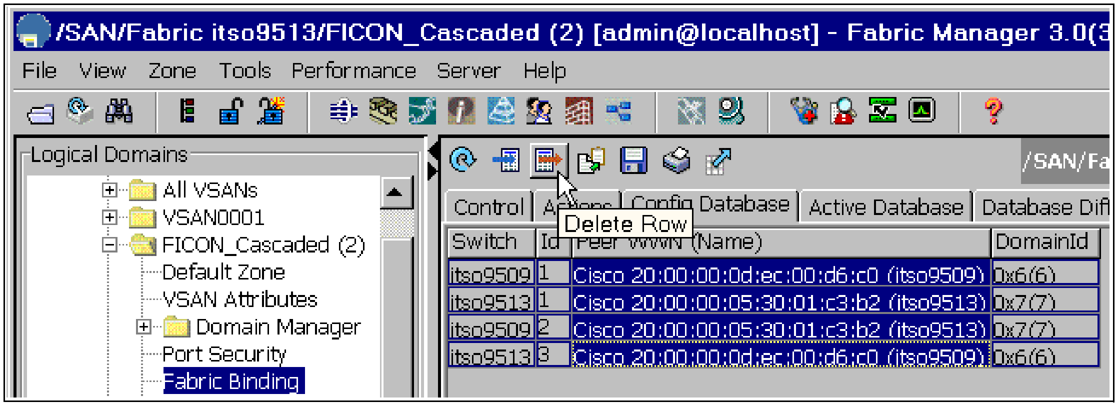
Switch	Status
itso9513	enabled

Figure 4-169 Fabric binding status of VSAN 3

From these displays you can see that fabric binding is enabled, and it was done as part of the FICON VSAN creation process. The next step is to configure the fabric binding database for VSAN 2, verify it, and activate it.

> **Note:** This is can be automatically done by the FM FICON VSAN Create wizard.

The currently configured database is shown in Figure 4-170.


/SAN/Fabric itso9513/FICON_Cascaded (2) [admin@localhost] - Fabric Manager 3.0(3
File View Zone Tools Performance Server Help
Logical Domains
All VSANs
VSAN0001
FICON_Cascaded (2)
Default Zone
VSAN Attributes
Domain Manager
Port Security
Fabric Binding
/SAN/Fa
Control
Actions
Config Database
Active Database
Database Diff
Delete Row

Switch	Id	Peer WWN (Name)	DomainId
itso9509	1	Cisco 20:00:00:0d:ec:00:d6:c0 (itso9509)	0x6(6)
itso9513	1	Cisco 20:00:00:05:30:01:c3:b2 (itso9513)	0x7(7)
itso9509	2	Cisco 20:00:00:05:30:01:c3:b2 (itso9513)	0x7(7)
itso9513	3	Cisco 20:00:00:0d:ec:00:d6:c0 (itso9509)	0x6(6)

Figure 4-170 Current Fabric Binding database for VSAN 10

As an example of how to remove entries, we show how to delete the entries, we hold the CTRL key down and left-click each entry as shown in Figure 4-170. When we have highlighted the entries, we can either then right-click and select Delete Row from the pull-down menu, or select the **Delete Row** icon.

After the entries are deleted, the next step is to create the new fabric binding entries with the updated domain IDs. To do this we select the **Create Row** icon at the top of the pane as shown in Figure 4-171.

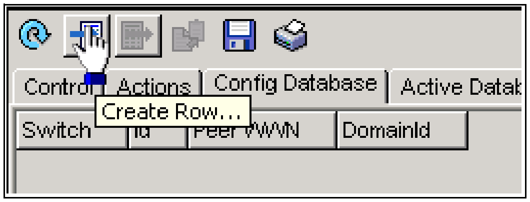
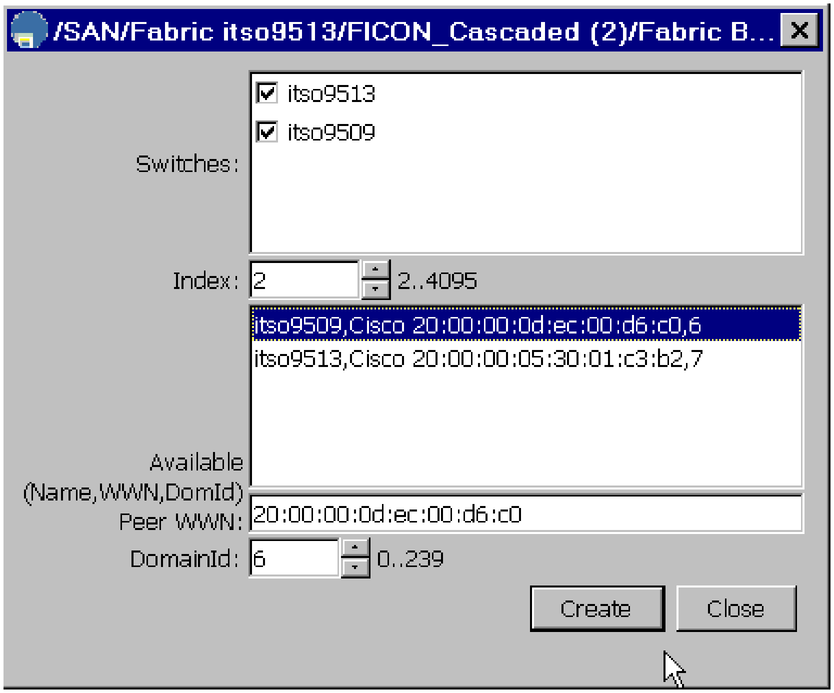

Control
Actions
Config Database
Active Datab
Create Row...
Switch
Id
Peer WWN
DomainId

Figure 4-171 Create new fabric binding entries

This opens another window where we can select which WWNs we want to add to the fabric binding configuration database. In Figure 4-171 we are adding the 9509 to the fabric binding database of both switches.


/SAN/Fabric itso9513/FICON_Cascaded (2)/Fabric B...

Switches:
☑ itso9513
☑ itso9509

Index: 2 2..4095

Available (Name,WWN,DomId):
itso9509,Cisco 20:00:00:0d:ec:00:d6:c0,6
itso9513,Cisco 20:00:00:05:30:01:c3:b2,7

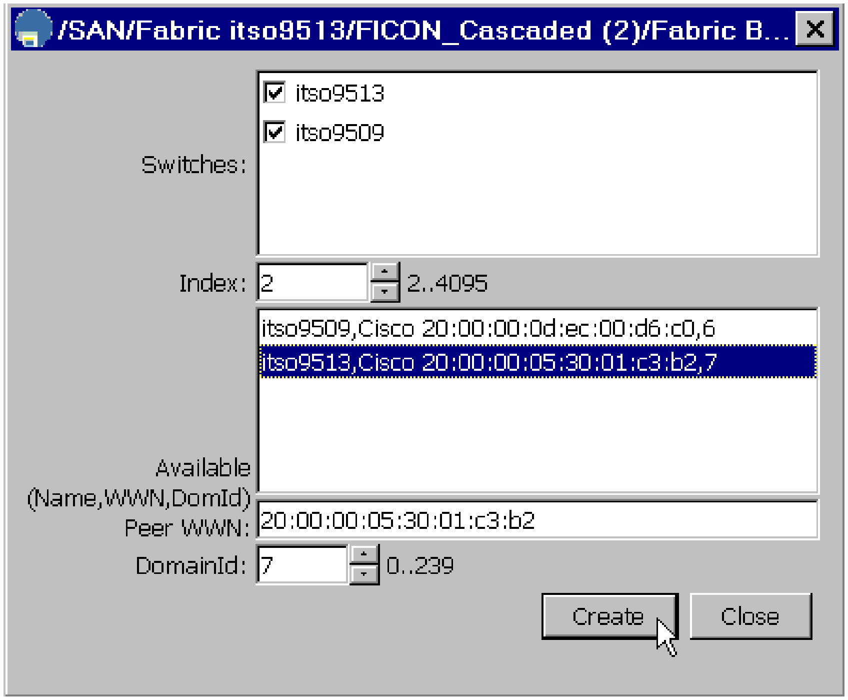
Peer WWN: 20:00:00:0d:ec:00:d6:c0

DomainId: 6 0..239

Create
Close

Figure 4-172 Creation of the fabric binding entry for the 9513 on both switches

In Figure 4-173 we are adding the 9513 to the fabric binding database of both switches.


/SAN/Fabric itso9513/FICON_Cascaded (2)/Fabric B...
Create
Close

Switches:
☑ itso9513
☑ itso9509

Index: 2 2..4095

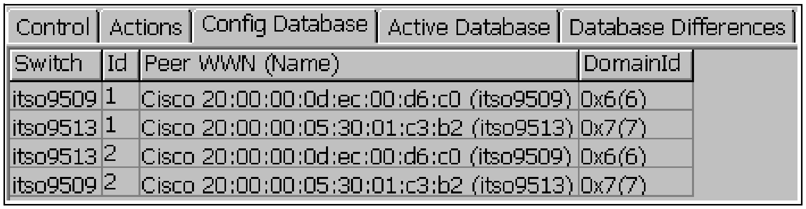
Available (Name,WWN,DomId):
itso9509,Cisco 20:00:00:0d:ec:00:d6:c0,6
itso9513,Cisco 20:00:00:05:30:01:c3:b2,7

Peer WWN: 20:00:00:05:30:01:c3:b2

DomainId: 7 0..239

Figure 4-173 Creation of the fabric binding entry for the 9506 on both switches

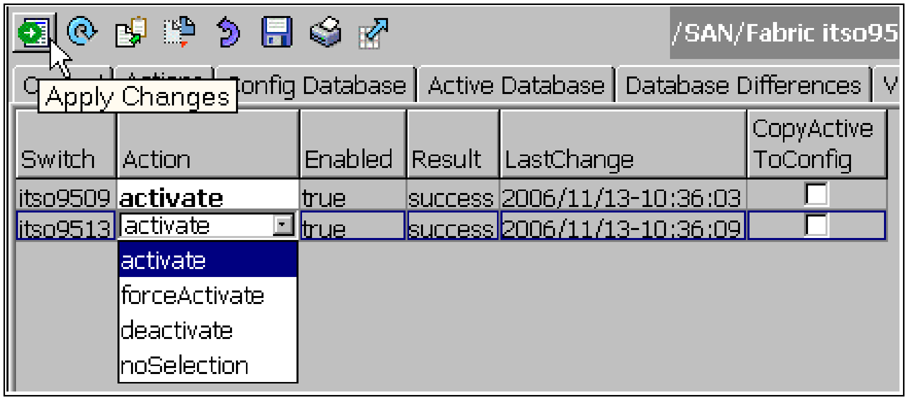
In Figure 4-174 we verify the newly configured fabric binding database to confirm its accuracy by selecting the **Config Database** tab.


Control
Actions
Config Database
Active Database
Database Differences

Switch	Id	Peer WWN (Name)	DomainId
itso9509	1	Cisco 20:00:00:0d:ec:00:d6:c0 (itso9509)	0x6(6)
itso9513	1	Cisco 20:00:00:05:30:01:c3:b2 (itso9513)	0x7(7)
itso9513	2	Cisco 20:00:00:0d:ec:00:d6:c0 (itso9509)	0x6(6)
itso9509	2	Cisco 20:00:00:05:30:01:c3:b2 (itso9513)	0x7(7)

Figure 4-174 New fabric binding entries

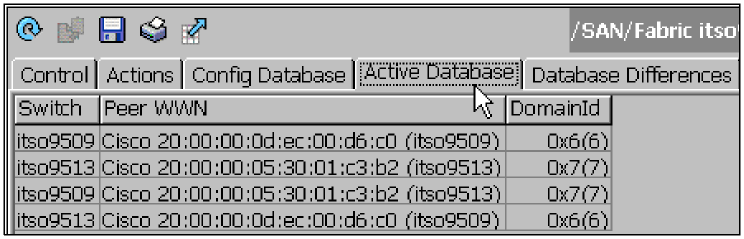
The next step in this process is to activate the newly defined configuration database. This is done by selecting the **Actions** tab, click in the **Action** column for each switch and select **activate** from the pull-down selection list, then click the **Apply Changes** icon as shown in Figure 4-175.


/SAN/Fabric itso95
Apply Changes
onfig Database
Active Database
Database Differences
activate
forceActivate
deactivate
noSelection

Switch	Action	Enabled	Result	LastChange	CopyActive ToConfig
itso9509	**activate**	true	success	2006/11/13-10:36:03	☐
itso9513	activate	true	success	2006/11/13-10:36:09	☐

Figure 4-175 Activate new fabric binding database

The active fabric binding database now looks correct, like that shown in Figure 4-176.


/SAN/Fabric itso
Control
Actions
Config Database
Active Database
Database Differences

Switch	Peer WWN	DomainId
itso9509	Cisco 20:00:00:0d:ec:00:d6:c0 (itso9509)	0x6(6)
itso9513	Cisco 20:00:00:05:30:01:c3:b2 (itso9513)	0x7(7)
itso9509	Cisco 20:00:00:05:30:01:c3:b2 (itso9513)	0x7(7)
itso9513	Cisco 20:00:00:0d:ec:00:d6:c0 (itso9509)	0x6(6)

Figure 4-176 Current active fabric binding database

4.17 PortChannel configuration

PortChannels refer to the aggregation of multiple physical interfaces into one logical interface to provide higher aggregated bandwidth, load balancing, and link redundancy. It is recommended that PortChannels be built using interfaces across multiple switching modules so that a failure in one module does not bring down the PortChannel link.

In summary, PortChannels provide increased reliability and performance by:

- Combining multiple ISLs into a single logical link.
- Aggregating bandwidth by distributing traffic among all functional links in the PortChannel.

- Providing high availability. If one physical link fails, traffic previously carried on this link is switched to the remaining links. If a link goes down in a PortChannel, the upper protocol is not aware of it. To the upper protocol, the link is still there, although the bandwidth is diminished. The routing tables are not affected by link failure. PortChannels can contain up to 16 physical links and can span multiple modules for added high availability.

We create our PortChannel configuration by using the PortChannel Wizard inside FM, but in order to use this wizard, the ISLs between the switch must be currently up and active. Remember that this was done prior to the creation of the FICON VSANs discussed in “FICON VSAN configuration and requirements” on page 890. Refer to that section for details of how to activate the ISLs.

When we have verified that both ISLs have come online, we can select the PortChannel wizard icon as shown in Figure 4-177.

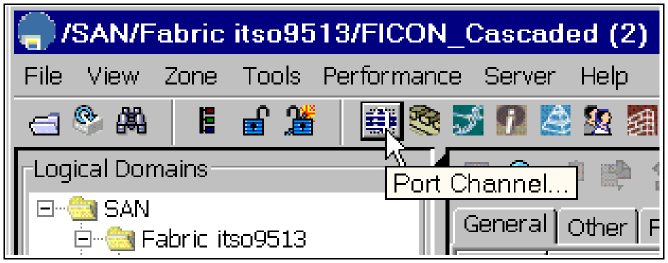
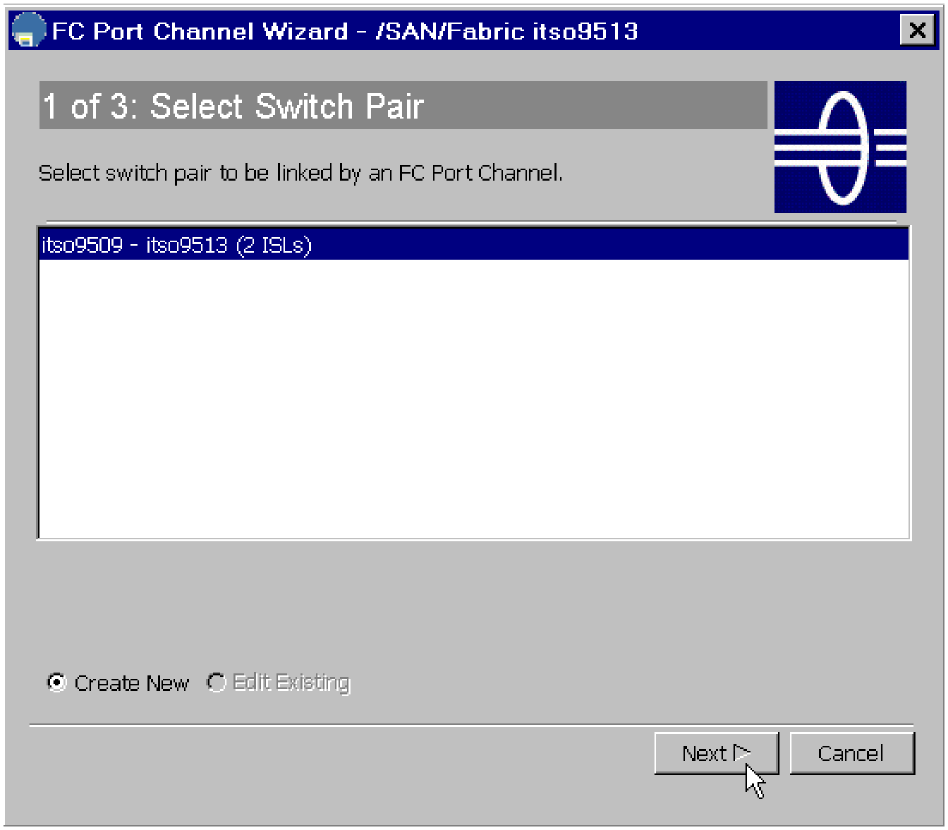

/SAN/Fabric itso9513/FICON_Cascaded (2)
File
View
Zone
Tools
Performance
Server
Help
Logical Domains
Port Channel...
SAN
Fabric itso9513
General
Other

Figure 4-177 PortChannel Wizard in FM

This brings up the PortChannel Wizard series of panels. In the first panel, Figure 4-178 we select the switches we want to create the PortChannel between (itso9509 and itso9513). Select **Create New** and click **Next**.


FC Port Channel Wizard - /SAN/Fabric itso9513
1 of 3: Select Switch Pair

Select switch pair to be linked by an FC Port Channel.

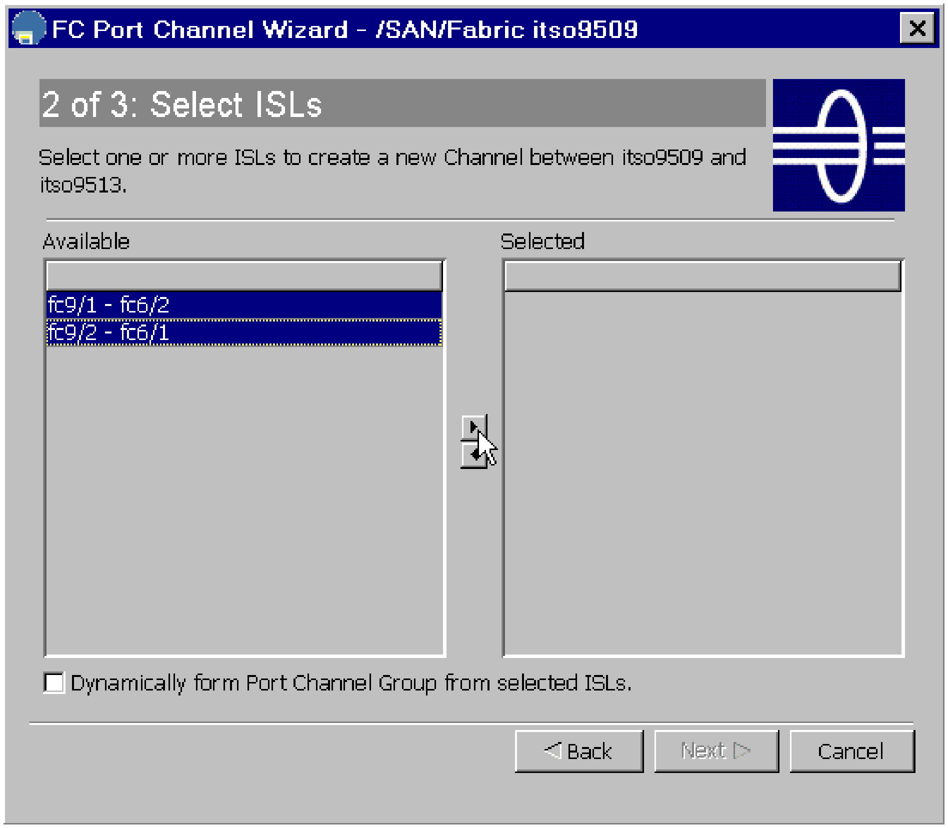
itso9509 - itso9513 (2 ISLs)

● Create New ○ Edit Existing

Next
Cancel

Figure 4-178 PortChannel panel 1 of 3

The next panel, Figure 4-179, is where we select the ISLs we want to bundle into the PortChannel. It is best practice to select links from multiple modules for high availability reasons. In our case, we did not have this luxury and we selected ISLs that were connected to ports 9/1 and 9/2 on the 9509, and ports 6/1 and 6/2 on the 9513. We then used the right arrow icon to move the ISLs from the **Available** column to the **Selected** column.


FC Port Channel Wizard - /SAN/Fabric itso9509
2 of 3: Select ISLs

Select one or more ISLs to create a new Channel between itso9509 and itso9513.

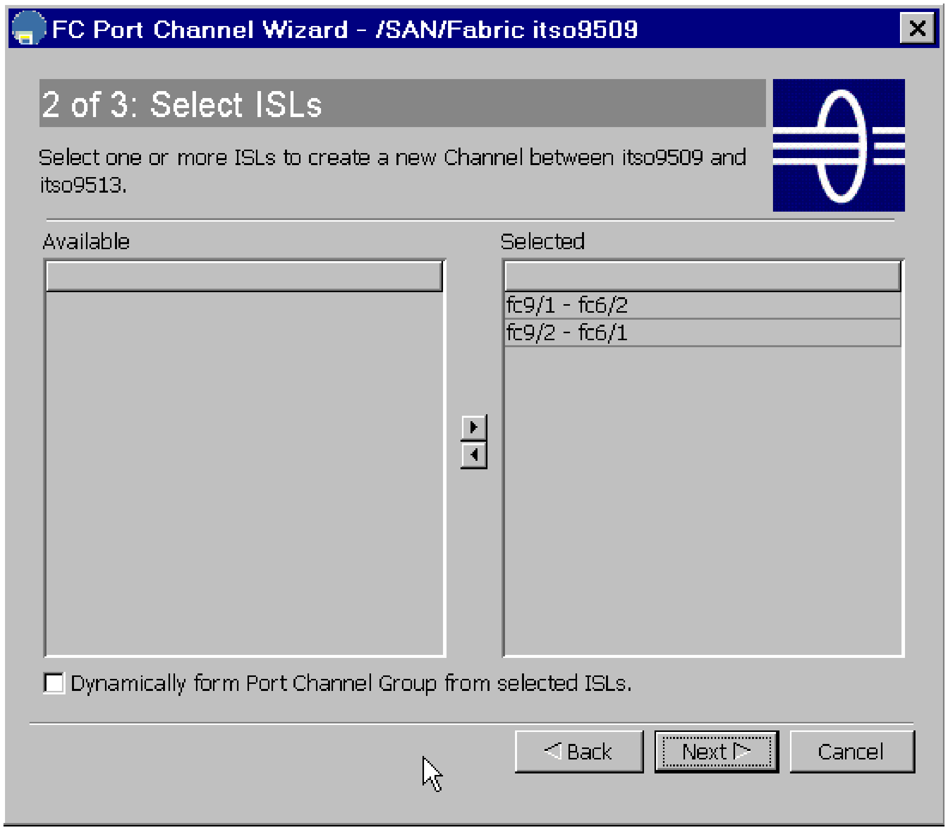
Available
fc9/1 - fc6/2
fc9/2 - fc6/1
Selected

☐ Dynamically form Port Channel Group from selected ISLs.

◁ Back
Next ▷
Cancel

Figure 4-179 PortChannel ISL selection panel

We have not checked the box to Dynamically form Port Channel Group from selected ISLs. We want to select the FICON Port address ourselves; so to proceed with the configuration of the PortChannel we selected **Next**, as shown in Figure 4-180.


FC Port Channel Wizard - /SAN/Fabric itso9509

2 of 3: Select ISLs

Select one or more ISLs to create a new Channel between itso9509 and itso9513.

Selected:

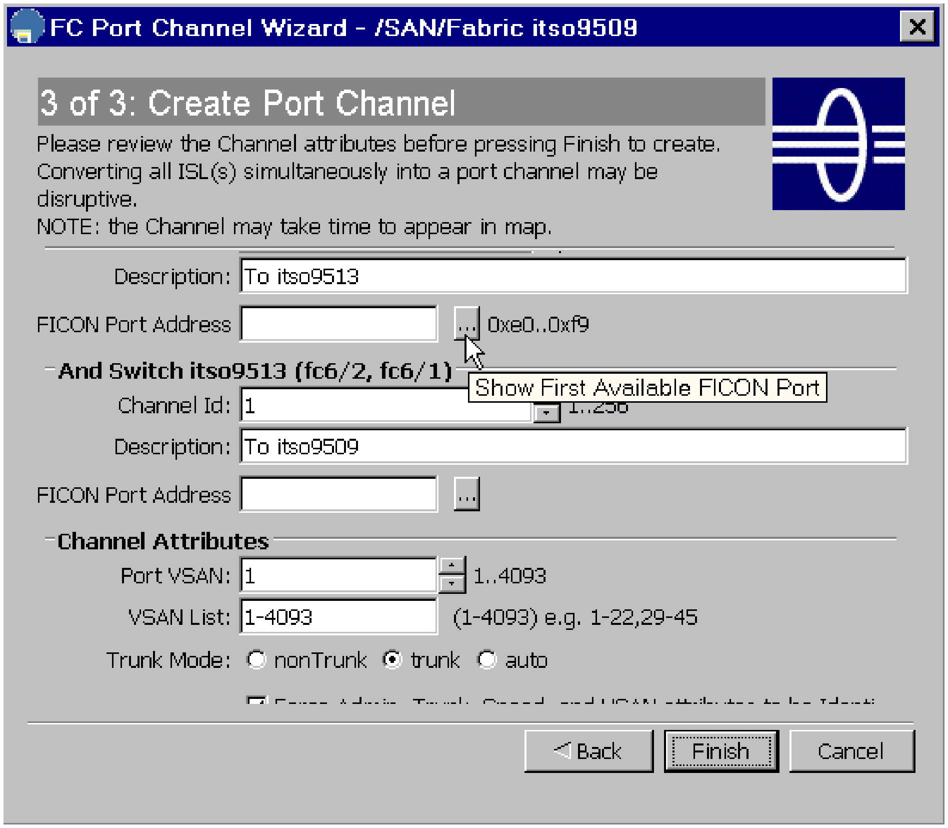
fc9/1 - fc6/2
fc9/2 - fc6/1

☐ Dynamically form Port Channel Group from selected ISLs.

Figure 4-180 PortChannel ISL selection panel 2

Panel 3 of the PortChannel wizard, Figure 4-181, is where we can set the attributes of the PortChannel. The following attributes can be set:

- Channel ID number.
- Description of the PortChannel. The wizard puts in a default description of the destination if we do not enter a description. The configuration in both switches is updated with this description.
- FICON Port Address. To get the next available FICON port address, click the box shown in Figure 4-181.



FC Port Channel Wizard - /SAN/Fabric itso9509

3 of 3: Create Port Channel

Please review the Channel attributes before pressing Finish to create. Converting all ISL(s) simultaneously into a port channel may be disruptive.
NOTE: the Channel may take time to appear in map.

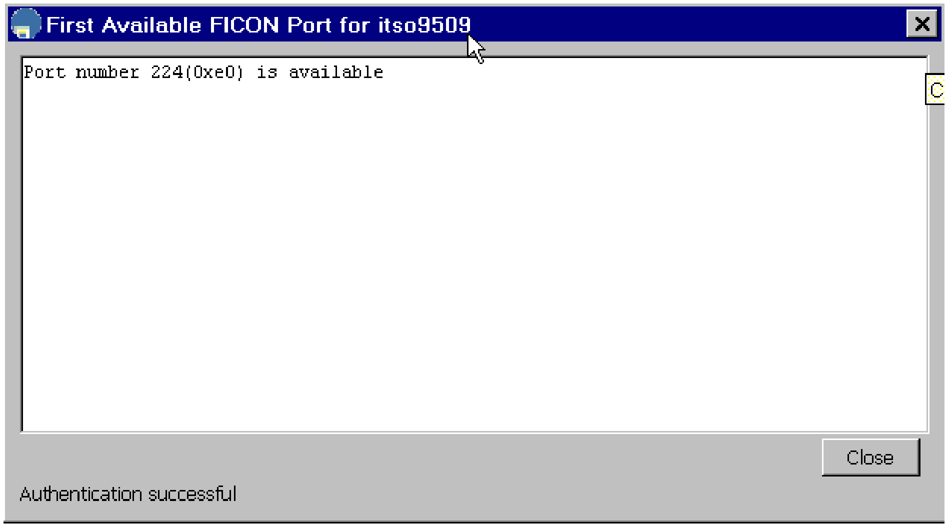
Description: To itso9513
FICON Port Address: 0xe0..0xf9

And Switch itso9513 (fc6/2, fc6/1)
Channel Id: 1 1..256
Description: To itso9509
FICON Port Address:

Channel Attributes
Port VSAN: 1 1..4093
VSAN List: 1-4093 (1-4093) e.g. 1-22,29-45
Trunk Mode: ○ nonTrunk ● trunk ○ auto

Figure 4-181 Show first available FICON port

Clicking **Show first available FICON port** gives you the pop-up menu shown in Figure 4-182.



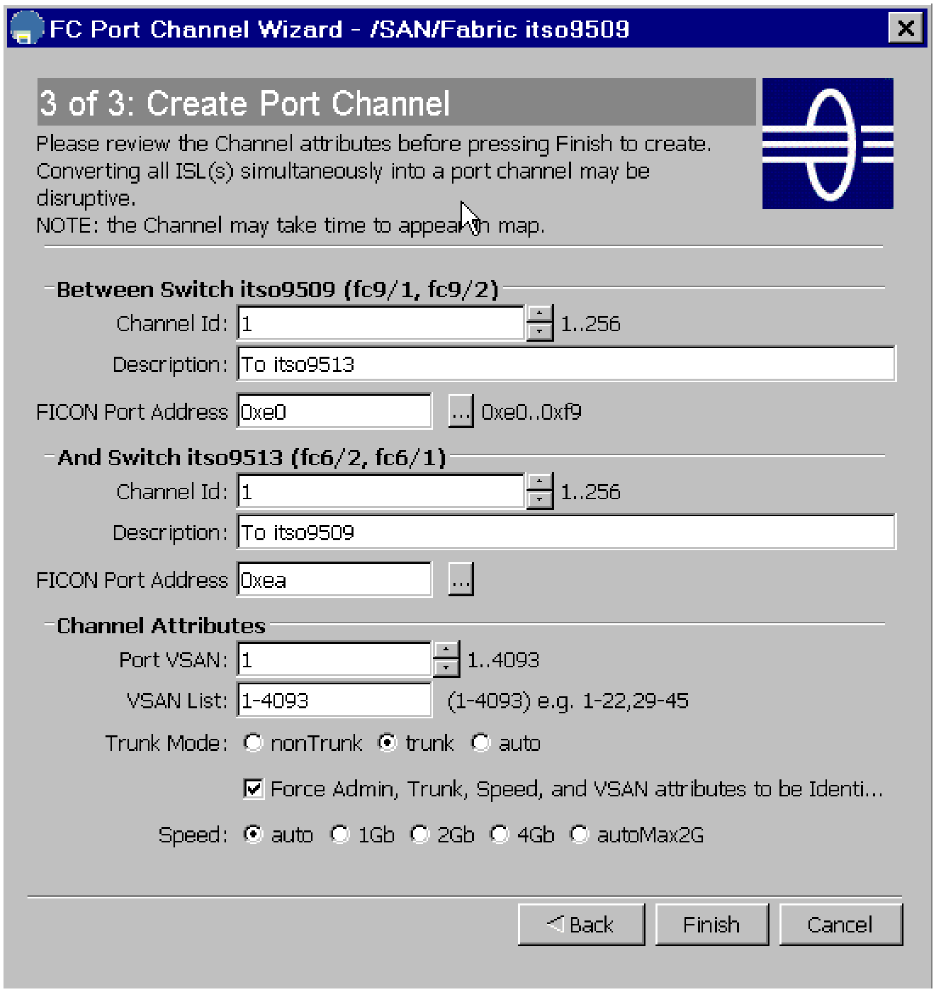
```
Port number 224(0xe0) is available
```

Authentication successful

Figure 4-182 First available FICON port

We enter the value 0xe0 into the field and repeat the same process for the next switch.

- We recommend that you leave the following check box selected: **Force admin trunk, speed, VSAN attributes to be identical**. Doing this helps to eliminate configuration errors.


FC Port Channel Wizard - /SAN/Fabric itso9509

3 of 3: Create Port Channel

Please review the Channel attributes before pressing Finish to create. Converting all ISL(s) simultaneously into a port channel may be disruptive.
NOTE: the Channel may take time to appear in map.

Between Switch itso9509 (fc9/1, fc9/2)

Channel Id: 1 1..256

Description: To itso9513

FICON Port Address 0xe0 0xe0..0xf9

And Switch itso9513 (fc6/2, fc6/1)

Channel Id: 1 1..256

Description: To itso9509

FICON Port Address 0xea

Channel Attributes

Port VSAN: 1 1..4093

VSAN List: 1-4093 (1-4093) e.g. 1-22,29-45

Trunk Mode: ○ nonTrunk ● trunk ○ auto

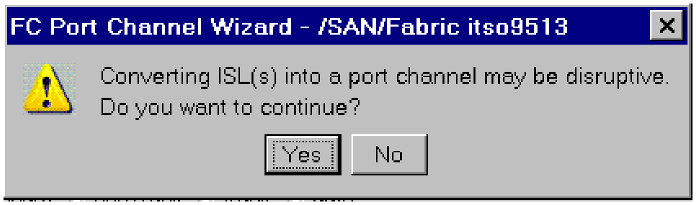
☑ Force Admin, Trunk, Speed, and VSAN attributes to be Identi...

Speed: ● auto ○ 1Gb ○ 2Gb ○ 4Gb ○ autoMax2G

< Back
Finish
Cancel

Figure 4-183 PortChannel wizard panel 3

The error message in Figure 4-184 warns us that moving ISLs into PortChannels is a disruptive operation.

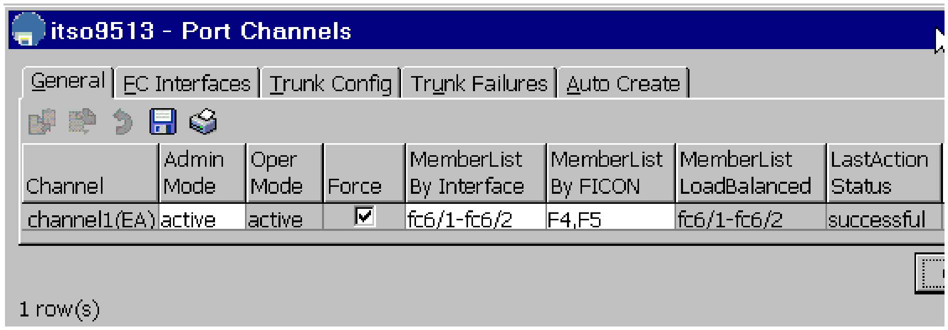

FC Port Channel Wizard - /SAN/Fabric itso9513

Converting ISL(s) into a port channel may be disruptive.
Do you want to continue?

Yes
No

Figure 4-184 PortChannel creation warning message

In DM, to verify the PortChannel operation, we selected **Interfaces →Port Channels** on the 9513 as shown in Figure 4-185.

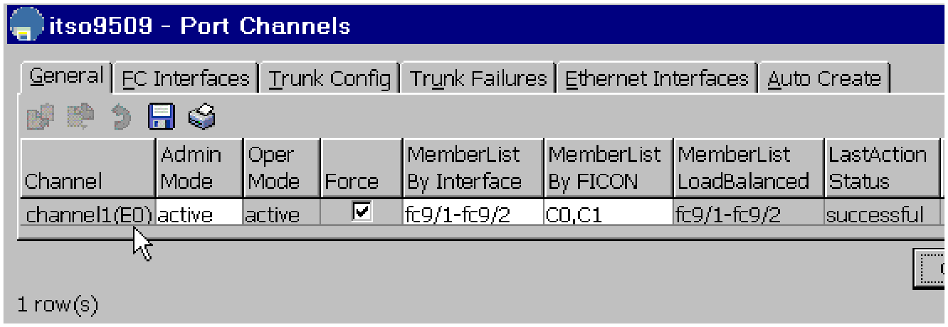

itso9513 - Port Channels
General
FC Interfaces
Trunk Config
Trunk Failures
Auto Create

Channel	Admin Mode	Oper Mode	Force	MemberList By Interface	MemberList By FICON	MemberList LoadBalanced	LastAction Status
channel1(EA)	active	active	☑	fc6/1-fc6/2	F4,F5	fc6/1-fc6/2	successful

1 row(s)

Figure 4-185 9513 Port Channel verification

We did the same on the 9509 as shown in Figure 4-186.

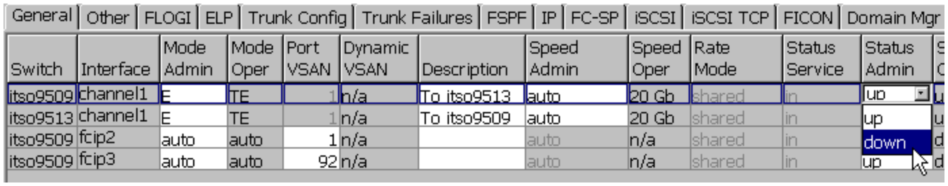

itso9509 - Port Channels
General
FC Interfaces
Trunk Config
Trunk Failures
Ethernet Interfaces
Auto Create

Channel	Admin Mode	Oper Mode	Force	MemberList By Interface	MemberList By FICON	MemberList LoadBalanced	LastAction Status
channel1(E0)	active	active	☑	fc9/1-fc9/2	C0,C1	fc9/1-fc9/2	successful

1 row(s)

Figure 4-186 9509 verification

If at any point you have to take down (known as *admin down*) and then bring back up (known as *admin up*) the logical PortChannel interface to cause a reinitialization to occur, this can be done in FM by selecting the **Physical Attributes** tab, open the **Switches →Interfaces** folders, and select **FC Logical** as shown in Figure 4-187.


General
Other
FLOGI
ELP
Trunk Config
Trunk Failures
FSPF
IP
FC-SP
iSCSI
iSCSI TCP
FICON
Domain Mgr

Switch	Interface	Mode Admin	Mode Oper	Port VSAN	Dynamic VSAN	Description	Speed Admin	Speed Oper	Rate Mode	Status Service	Status Admin
itso9509	channel1	E	TE	1	n/a	To itso9513	auto	20 Gb	shared	in	up
itso9513	channel1	E	TE	1	n/a	To itso9509	auto	20 Gb	shared	in	up
itso9509	fcip2	auto	auto	1	n/a		auto	n/a	shared	in	down
itso9509	fcip3	auto	auto	92	n/a		auto	n/a	shared	in	up

Figure 4-187 Reinitialization

From the **General** tab, **Admin down** the PortChannel in question, and **Apply** the changes. To **Admin up** the PortChannel, select **up** and **Apply** the changes.

It takes a while for FM to display the changes, so we use the CLI **`sho int port-channel`** command on both the 9509 and the 9513 to verify that all is well, as shown in Example 4-31 and Example 4-32.

Example 4-31 9509 display

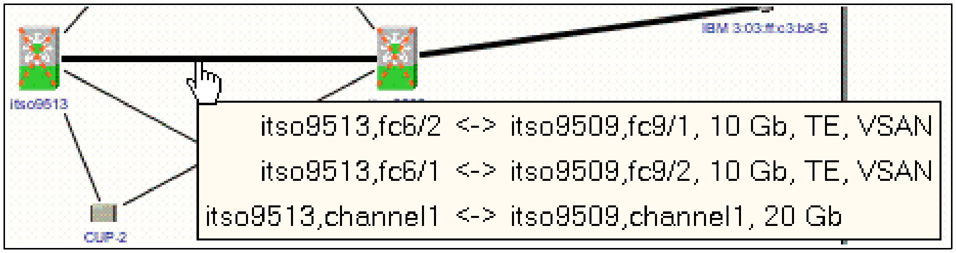
```
itso9509# sho int port-channel 1
port-channel 1 is trunking
    Port description is To itso9513
    Hardware is Fibre Channel
    Port WWN is 24:01:00:0d:ec:00:d6:c0
    Admin port mode is E, trunk mode is on
    snmp traps are enabled
    Port mode is TE
    Port vsan is 1
    Speed is 20 Gbps
    Trunk vsans (admin allowed and active) (1-2,92-94)
    Trunk vsans (up)                       (1-2,92-94)
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             ()
    5 minutes input rate 13608 bits/sec, 1701 bytes/sec, 21 frames/sec
    5 minutes output rate 12808 bits/sec, 1601 bytes/sec, 19 frames/sec
      6670 frames input, 502336 bytes
        0 discards, 0 errors
        0 CRC,  0 unknown class
        0 too long, 0 too short
      5927 frames output, 461048 bytes
        0 discards, 0 errors
      0 input OLS, 2 LRR, 0 NOS, 0 loop inits
      3 output OLS, 2 LRR, 0 NOS, 0 loop inits
--More--
```

Example 4-32 9513 display

```
   itso9513# sho int port-channel 1
   port-channel 1 is trunking
       Port description is To itso9509
       Hardware is Fibre Channel
       Port WWN is 24:01:00:05:30:01:c3:b2
       Admin port mode is E, trunk mode is on
       snmp traps are enabled
       Port mode is TE
       Port vsan is 1
       Speed is 20 Gbps
       Trunk vsans (admin allowed and active) (1-2,92-94)
       Trunk vsans (up)                       (1-2,92-94)
```

```
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             ()
    5 minutes input rate 2440 bits/sec, 305 bytes/sec, 1 frames/sec
    5 minutes output rate 808 bits/sec, 101 bytes/sec, 1 frames/sec
      6517 frames input, 599860 bytes
        0 discards, 0 errors
        0 CRC,  0 unknown class
        0 too long, 0 too short
      7205 frames output, 542860 bytes
        0 discards, 0 errors
      2 input OLS, 2 LRR, 2 NOS, 0 loop inits
      2 output OLS, 2 LRR, 0 NOS, 0 loop inits
--More--
```

To use FM to display the ISL/PortChannel operation, we hover our cursor on the ISL between itso9509 and itso9513 in the SAN fabric map as shown in Figure 4-188.



itso9513,fc6/2 <-> itso9509,fc9/1, 10 Gb, TE, VSAN
itso9513,fc6/1 <-> itso9509,fc9/2, 10 Gb, TE, VSAN
itso9513,channel1 <-> itso9509,channel1, 20 Gb

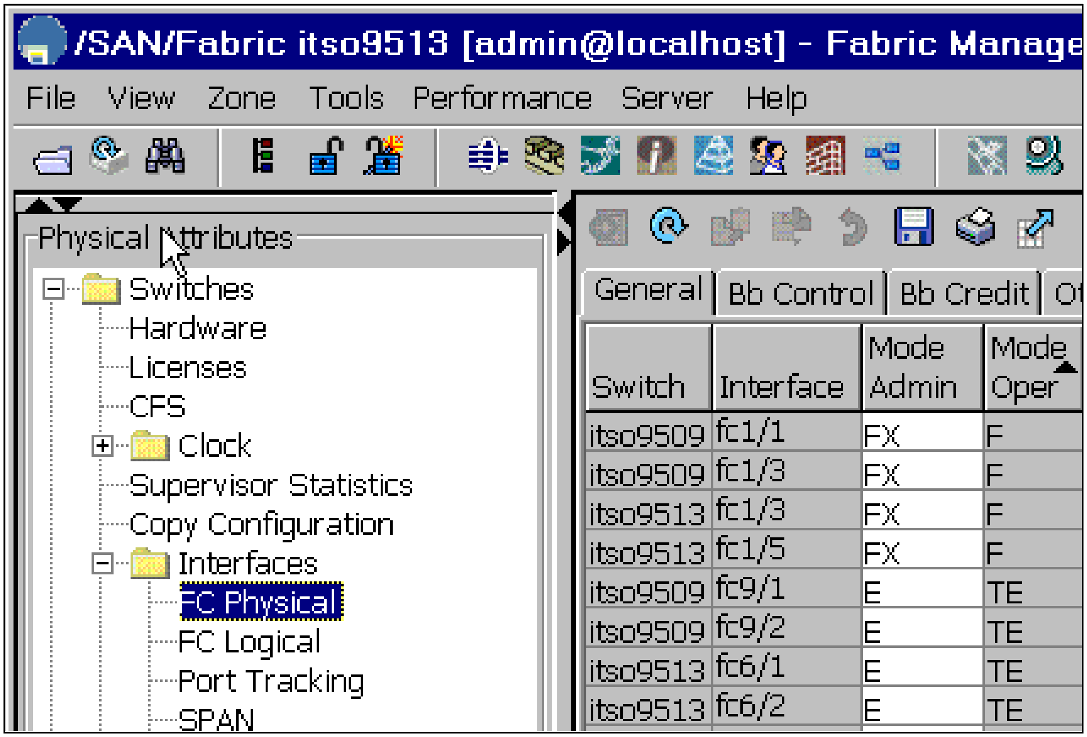
Figure 4-188 FM ISL display

4.18 Moving ports to the FICON VSAN

At this point, the last remaining FICON switch configuration step is to move all the required ports for the channels and control units into the correct FICON VSANs and enable the ports. Remember that FICON VSAN 5 was defined on the 122 switch, and FICON VSAN 10 on the 81 and 49 switches. We have to perform this operation once for *each* fabric.

Previously we used DM to enable the ISL ports; for this section we use FM to configure and enable ports. To accomplish this, we select the **Physical Attributes** tab in FM and open the **Switches** → **Interfaces** folder, and select **FC Physical** as shown in Figure 4-189.

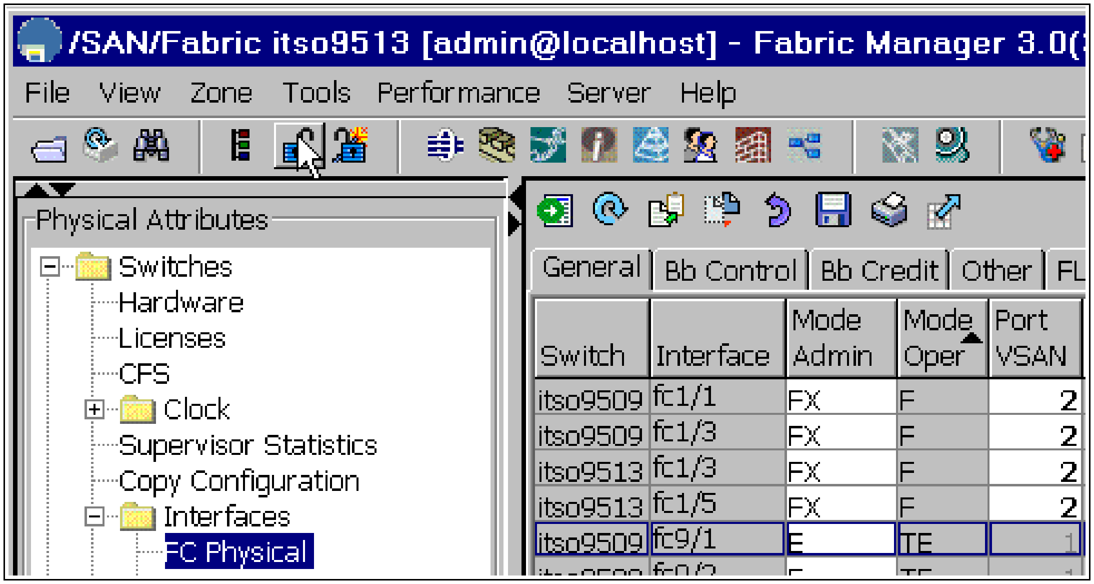
We select the **General** tab in the right information pane above the FM map, and we see the panel shown in Figure 4-189. We can sort on any column by clicking it once.


/SAN/Fabric itso9513 [admin@localhost] - Fabric Manage
File
View
Zone
Tools
Performance
Server
Help
Physical Attributes
Switches
Hardware
Licenses
CFS
Clock
Supervisor Statistics
Copy Configuration
Interfaces
FC Physical
FC Logical
Port Tracking
SPAN
General
Bb Control
Bb Credit
Ot

Switch	Interface	Mode Admin	Mode Oper
itso9509	fc1/1	FX	F
itso9509	fc1/3	FX	F
itso9513	fc1/3	FX	F
itso9513	fc1/5	FX	F
itso9509	fc9/1	E	TE
itso9509	fc9/2	E	TE
itso9513	fc6/1	E	TE
itso9513	fc6/2	E	TE

Figure 4-189 General tab of FM physical interface display

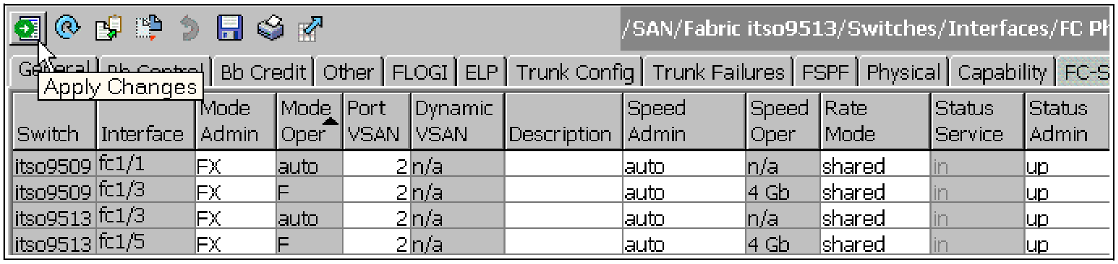
The next step is to place the ports we are using into the VSAN we want them in (in our case we change from VSAN 92 to VSAN 2), set them to **Admin Up** status (if not up already) as shown in Figure 4-190 and Figure 4-191, and apply the changes.


/SAN/Fabric itso9513 [admin@localhost] - Fabric Manager 3.0(
File
View
Zone
Tools
Performance
Server
Help
Physical Attributes
Switches
Hardware
Licenses
CFS
Clock
Supervisor Statistics
Copy Configuration
Interfaces
FC Physical
General
Bb Control
Bb Credit
Other
FL

Switch	Interface	Mode Admin	Mode Oper	Port VSAN
itso9509	fc1/1	FX	F	2
itso9509	fc1/3	FX	F	2
itso9513	fc1/3	FX	F	2
itso9513	fc1/5	FX	F	2
itso9509	fc9/1	E	TE	1

Figure 4-190 Ports on the 9509 that we want to change

In Figure 4-191 we click **Apply Changes**.


/SAN/Fabric itso9513/Switches/Interfaces/FC Ph
General
Bb Control
Apply Changes
Bb Credit
Other
FLOGI
ELP
Trunk Config
Trunk Failures
FSPF
Physical
Capability
FC-S

Switch	Interface	Mode Admin	Mode Oper	Port VSAN	Dynamic VSAN	Description	Speed Admin	Speed Oper	Rate Mode	Status Service	Status Admin
itso9509	fc1/1	FX	auto	2	n/a		auto	n/a	shared	in	up
itso9509	fc1/3	FX	F	2	n/a		auto	4 Gb	shared	in	up
itso9513	fc1/3	FX	auto	2	n/a		auto	n/a	shared	in	up
itso9513	fc1/5	FX	F	2	n/a		auto	4 Gb	shared	in	up

Figure 4-191 Ports on the 9513 we want to change

Note: You have to repeat this process for the switch.

4.18.1 CUP management

The Control Unit Port (CUP) protocol configures access control and provides unified storage management capabilities from a mainframe computer. Cisco MDS 9000 FICON-enabled switches are fully IBM CUP standard compliant for in-band management using the IBM S/A OS/390® I/O operations console.

CUP is supported by switches and directors in the Cisco MDS 9000 Family. The CUP function allows the mainframe to manage the Cisco MDS switches. Host communication includes control functions such as blocking and unblocking ports, as well as monitoring and error reporting functions.

In Figure 4-192 we start the process to set the default zone to permit.

Note: There is no necessity to explicitly zone the CUP devices; setting the default zone to permit should be sufficient. However, we show the process in case you have to explicitly zone it.

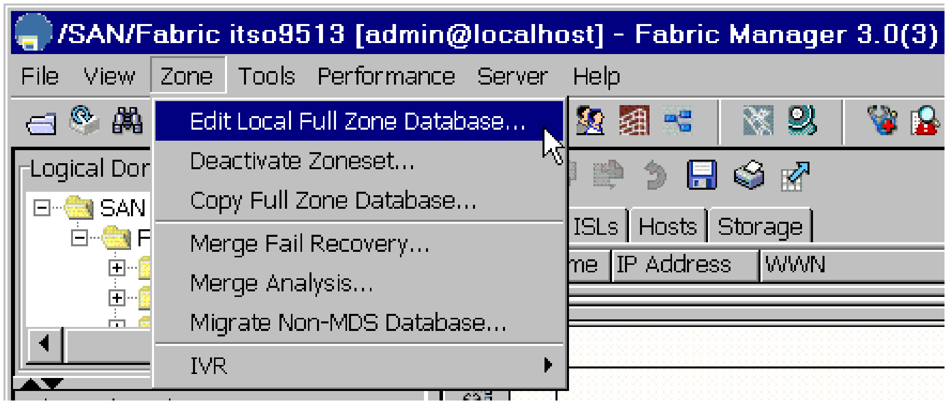

/SAN/Fabric itso9513 [admin@localhost] - Fabric Manager 3.0(3)
File
View
Zone
Tools
Performance
Server
Help
Edit Local Full Zone Database...
Deactivate Zoneset...
Copy Full Zone Database...
Merge Fail Recovery...
Merge Analysis...
Migrate Non-MDS Database...
IVR
Logical Dor
SAN
ISLs
Hosts
Storage
IP Address
WWN

Figure 4-192 Edit Local Full Zone Database

Figure 4-193 shows how we edit the default zone attributes from the Edit Local Full Zone Database Edit dropdown.

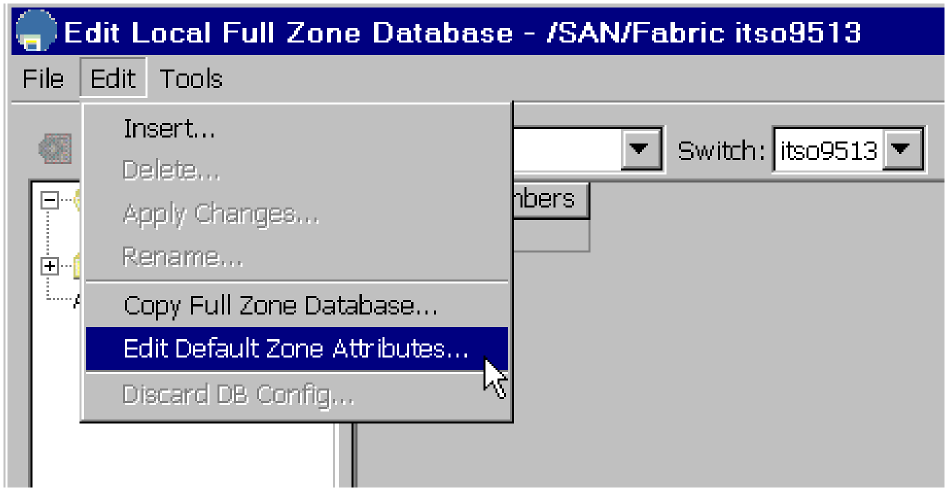
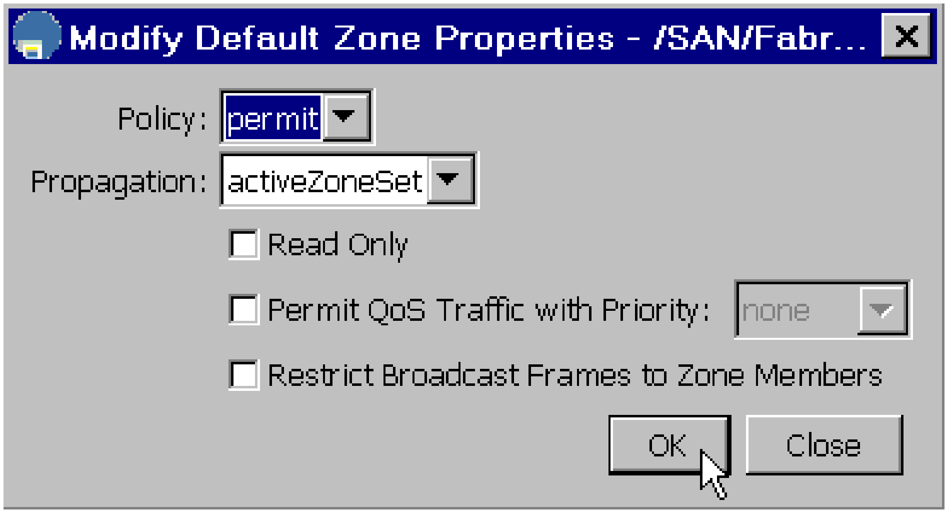

Edit Local Full Zone Database - /SAN/Fabric itso9513
File
Edit
Tools
Insert...
Delete...
Apply Changes...
Rename...
Copy Full Zone Database...
Edit Default Zone Attributes...
Discard DB Config...
Switch:
itso9513
nbers

Figure 4-193 Edit Default Zone Attributes

In Figure 4-194 we set the policy to permit if it is not already set and click **OK**.


Modify Default Zone Properties - /SAN/Fabr...
OK
Close

Policy: permit

Propagation: activeZoneSet

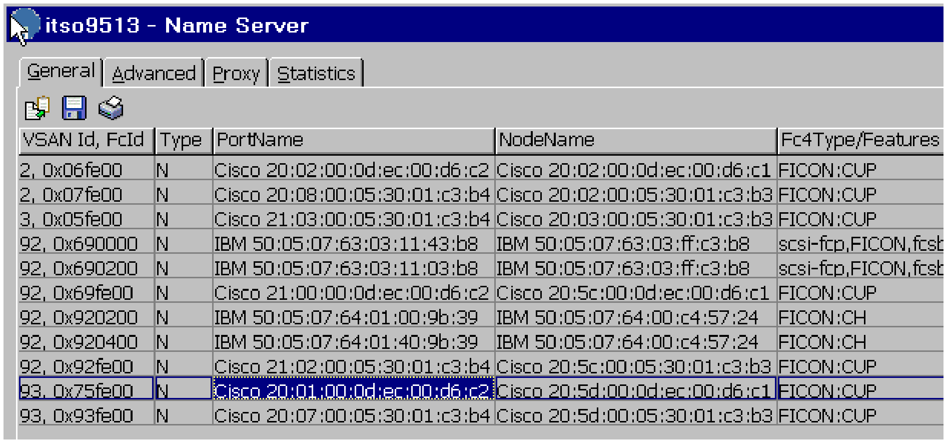
☐ Read Only

☐ Permit QoS Traffic with Priority: none

☐ Restrict Broadcast Frames to Zone Members

Figure 4-194 Modifying properties

In Figure 4-195 from **Device Manager** → **FC** → **Name Server** for our VSAN (93 in this case) we obtain the FICON:CUP WWN.



itso9513 - Name Server

General | Advanced | Proxy | Statistics

VSAN Id, FcId	Type	PortName	NodeName	Fc4Type/Features
2, 0x06fe00	N	Cisco 20:02:00:0d:ec:00:d6:c2	Cisco 20:02:00:0d:ec:00:d6:c1	FICON:CUP
2, 0x07fe00	N	Cisco 20:08:00:05:30:01:c3:b4	Cisco 20:02:00:05:30:01:c3:b3	FICON:CUP
3, 0x05fe00	N	Cisco 21:03:00:05:30:01:c3:b4	Cisco 20:03:00:05:30:01:c3:b3	FICON:CUP
92, 0x690000	N	IBM 50:05:07:63:03:11:43:b8	IBM 50:05:07:63:03:ff:c3:b8	scsi-fcp,FICON,fcsb
92, 0x690200	N	IBM 50:05:07:63:03:11:03:b8	IBM 50:05:07:63:03:ff:c3:b8	scsi-fcp,FICON,fcsb
92, 0x69fe00	N	Cisco 21:00:00:0d:ec:00:d6:c2	Cisco 20:5c:00:0d:ec:00:d6:c1	FICON:CUP
92, 0x920200	N	IBM 50:05:07:64:01:00:9b:39	IBM 50:05:07:64:00:c4:57:24	FICON:CH
92, 0x920400	N	IBM 50:05:07:64:01:40:9b:39	IBM 50:05:07:64:00:c4:57:24	FICON:CH
92, 0x92fe00	N	Cisco 21:02:00:05:30:01:c3:b4	Cisco 20:5c:00:05:30:01:c3:b3	FICON:CUP
93, 0x75fe00	N	Cisco 20:01:00:0d:ec:00:d6:c2	Cisco 20:5d:00:0d:ec:00:d6:c1	FICON:CUP
93, 0x93fe00	N	Cisco 20:07:00:05:30:01:c3:b4	Cisco 20:5d:00:05:30:01:c3:b3	FICON:CUP

Figure 4-195 Name Server

Next, in Figure 4-196, we edit the zone database for the FICON93 VSAN.

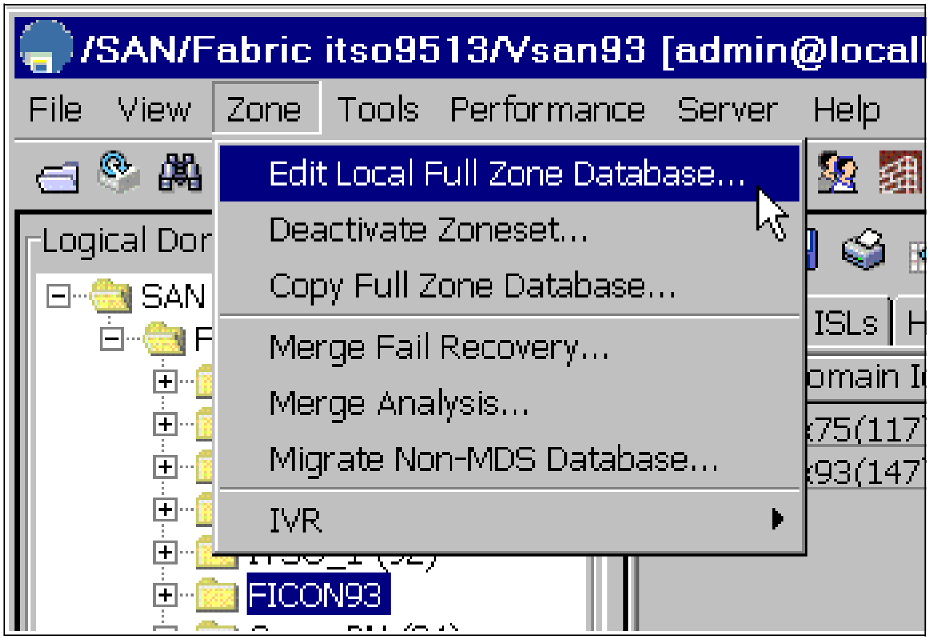
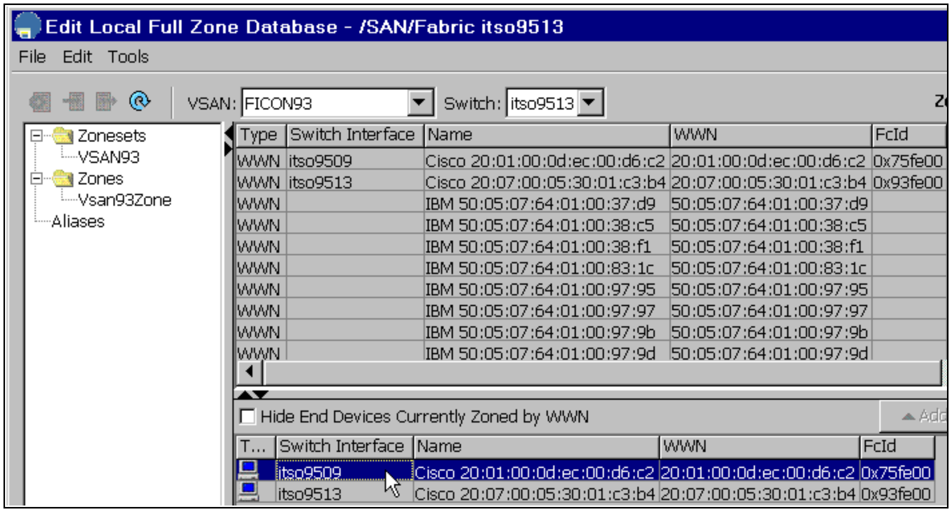

/SAN/Fabric itso9513/Vsan93 [admin@locall
File
View
Zone
Tools
Performance
Server
Help
Edit Local Full Zone Database...
Deactivate Zoneset...
Copy Full Zone Database...
Merge Fail Recovery...
Merge Analysis...
Migrate Non-MDS Database...
IVR
Logical Dor
SAN
F
FICON93
ISLs
omain I
75(117
93(147

Figure 4-196 FICON93

Figure 4-197 shows the zone after we have dragged and dropped itso9509 into the zone (which we identified in Figure 4-195 on page 923).

Important: If more than one FICON:CUP exists in this fabric, make sure to add all the FICON:CUP WWNs to the required zone.



VSAN: FICON93 Switch: itso9513

Type	Switch Interface	Name	WWN	FcId
WWN	itso9509	Cisco 20:01:00:0d:ec:00:d6:c2	20:01:00:0d:ec:00:d6:c2	0x75fe00
WWN	itso9513	Cisco 20:07:00:05:30:01:c3:b4	20:07:00:05:30:01:c3:b4	0x93fe00
WWN		IBM 50:05:07:64:01:00:37:d9	50:05:07:64:01:00:37:d9	
WWN		IBM 50:05:07:64:01:00:38:c5	50:05:07:64:01:00:38:c5	
WWN		IBM 50:05:07:64:01:00:38:f1	50:05:07:64:01:00:38:f1	
WWN		IBM 50:05:07:64:01:00:83:1c	50:05:07:64:01:00:83:1c	
WWN		IBM 50:05:07:64:01:00:97:95	50:05:07:64:01:00:97:95	
WWN		IBM 50:05:07:64:01:00:97:97	50:05:07:64:01:00:97:97	
WWN		IBM 50:05:07:64:01:00:97:9b	50:05:07:64:01:00:97:9b	
WWN		IBM 50:05:07:64:01:00:97:9d	50:05:07:64:01:00:97:9d	

☐ Hide End Devices Currently Zoned by WWN

T...	Switch Interface	Name	WWN	FcId
	itso9509	Cisco 20:01:00:0d:ec:00:d6:c2	20:01:00:0d:ec:00:d6:c2	0x75fe00
	itso9513	Cisco 20:07:00:05:30:01:c3:b4	20:07:00:05:30:01:c3:b4	0x93fe00

Figure 4-197 itso9509 dragged and dropped

4.19 Bringing CHPIDs, devices and CUP online

Now that we have configured the switches in both fabrics for FICON, you can start to bring the host ports (CHPIDS), the devices, and the CUP devices online. In DM for the 9513 we can see that the channel ports are online as shown in Figure 4-198.

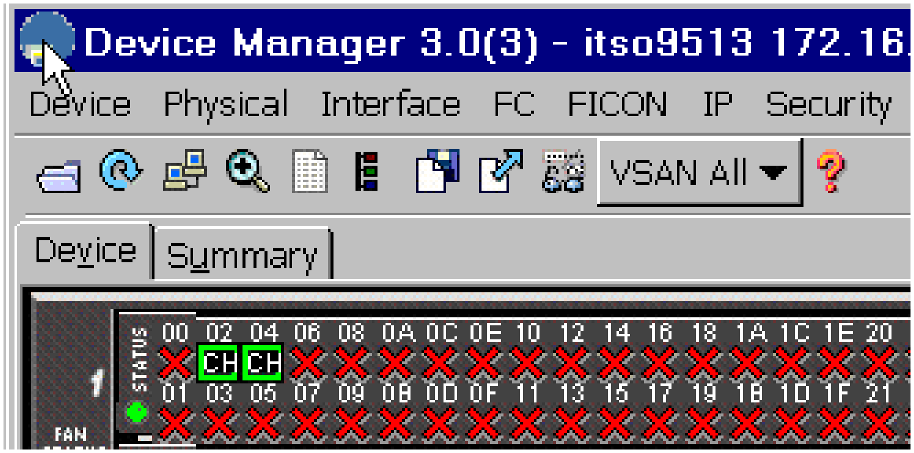

Device Manager 3.0(3) - itso9513 172.16.
Device
Physical
Interface
FC
FICON
IP
Security
VSAN All
Device
Summary
STATUS
00 02 04 06 08 0A 0C 0E 10 12 14 16 18 1A 1C 1E 20
CH CH
01 03 05 07 09 0B 0D 0F 11 13 15 17 19 1B 1D 1F 21
1
FAN

Figure 4-198 DM device view indicating channels online

We can see that the CUs are online in Figure 4-199.

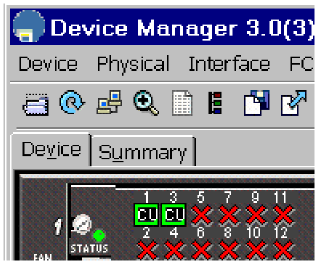
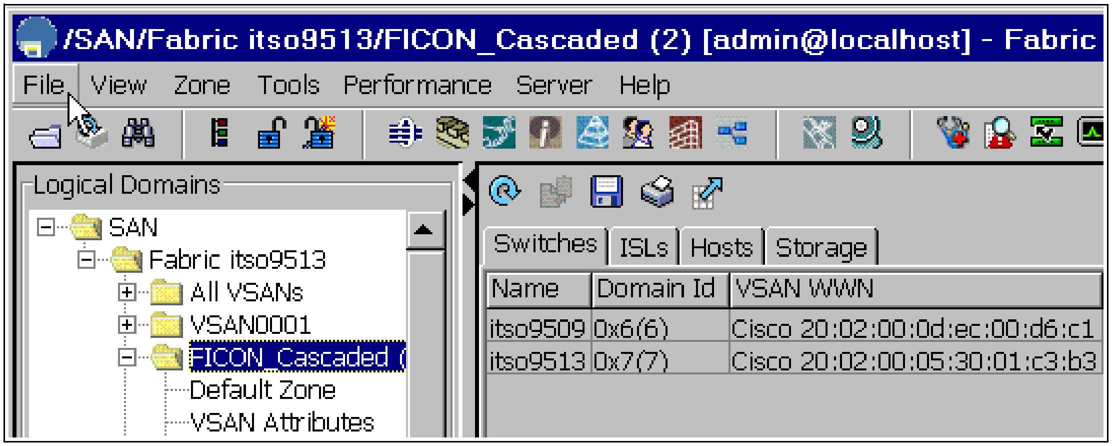

Device Manager 3.0(3)
Device
Physical
Interface
FC
Device
Summary
1 3 5 7 9 11
CU CU
2 4 6 8 10 12
1
STATUS
FAN

Figure 4-199 CUs online

Traditional open systems zoning can be done, but is unnecessary, because open systems and FICON traffic can be separated by VSAN. In our case, we are not using zoning and so we do not show zoning.

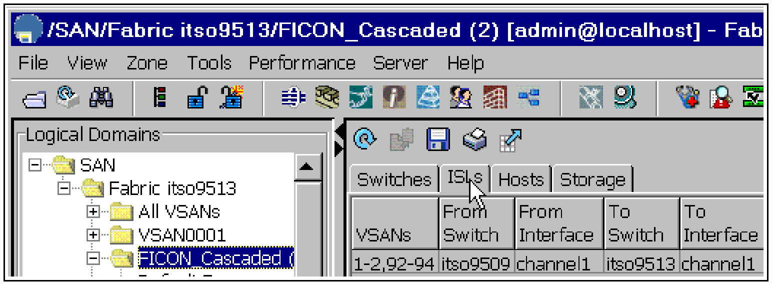
Figure 4-200 is a display of the switches that are part of the FICON cascaded VSAN.


/SAN/Fabric itso9513/FICON_Cascaded (2) [admin@localhost] - Fabric
File
View
Zone
Tools
Performance
Server
Help
Logical Domains
SAN
Fabric itso9513
All VSANs
VSAN0001
FICON_Cascaded (
Default Zone
VSAN Attributes
Switches
ISLs
Hosts
Storage

Name	Domain Id	VSAN WWN
itso9509	0x6(6)	Cisco 20:02:00:0d:ec:00:d6:c1
itso9513	0x7(7)	Cisco 20:02:00:05:30:01:c3:b3

Figure 4-200 FM display of the switches in FICON VSAN 2

In Figure 4-201 we can see summary information of the PortChannel defined between the 9509 and the 9513.


/SAN/Fabric itso9513/FICON_Cascaded (2) [admin@localhost] - Fab
File
View
Zone
Tools
Performance
Server
Help
Logical Domains
SAN
Fabric itso9513
All VSANs
VSAN0001
FICON_Cascaded (
Switches
ISLs
Hosts
Storage

VSANs	From Switch	From Interface	To Switch	To Interface
1-2,92-94	itso9509	channel1	itso9513	channel1

Figure 4-201 FM display of the PortChannel in VSAN 2

DM is used to manage an individual switch and FM is used to manage the fabric. In Figure 4-202 we show how to select the FICON Interface information.

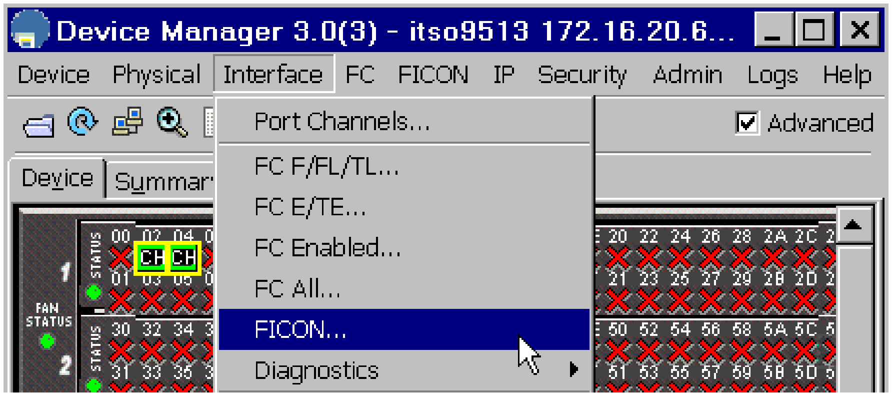
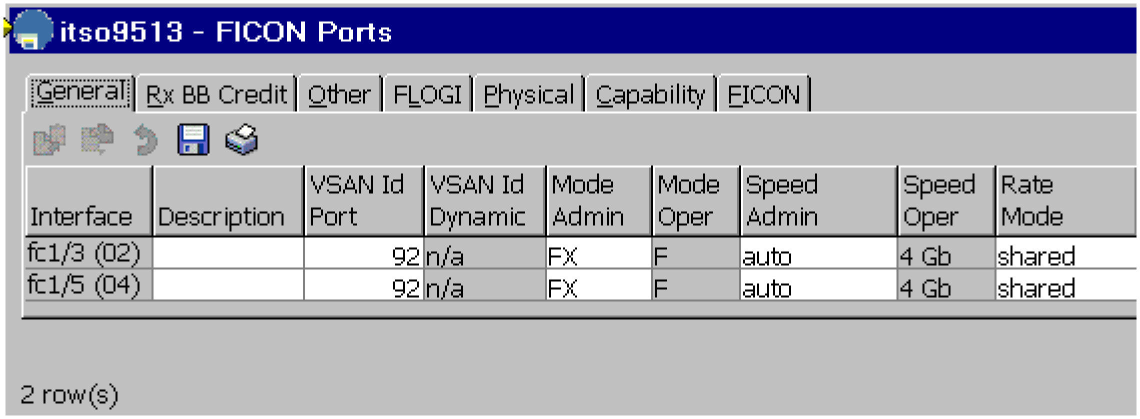

Device Manager 3.0(3) - itso9513 172.16.20.6...
Device
Physical
Interface
FC
FICON
IP
Security
Admin
Logs
Help
Advanced
Device
Summar
Port Channels...
FC F/FL/TL...
FC E/TE...
FC Enabled...
FC All...
FICON...
Diagnostics
FAN STATUS
STATUS
CH
CH

Figure 4-202 DM display showing both CH and CU ports online

Next, we look at the FICON interface information for this 9513.

The next display in Figure 4-203 provides us with the operational settings of the FICON ports.


itso9513 - FICON Ports
General
Rx BB Credit
Other
FLOGI
Physical
Capability
FICON

Interface	Description	VSAN Id Port	VSAN Id Dynamic	Mode Admin	Mode Oper	Speed Admin	Speed Oper	Rate Mode
fc1/3 (02)		92	n/a	FX	F	auto	4 Gb	shared
fc1/5 (04)		92	n/a	FX	F	auto	4 Gb	shared

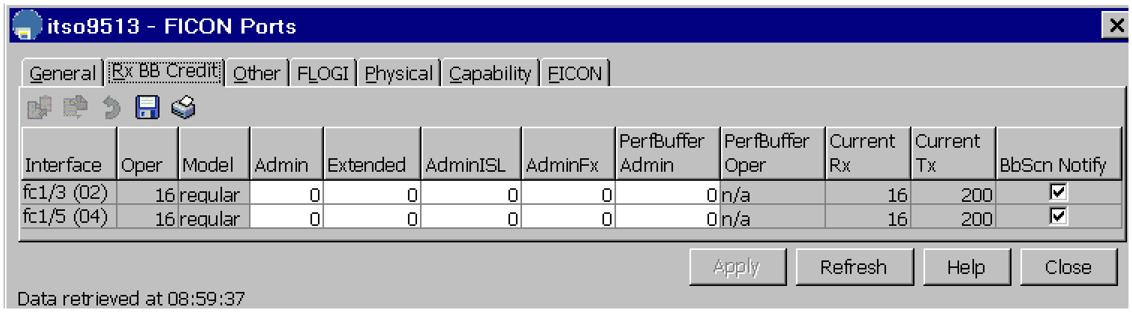
2 row(s)

Figure 4-203 DM display of FICON general information

Figure 4-204 is a display of the buffer-to-buffer BB credit information for the channel and control unit ports on the 9513.

The current **RX BB Credit** is the amount of frames the device can send to the switch without waiting for an R_RDY from the switch to replenish the BB credit. The **TX** value is the amount of frames the switch can send to the device without waiting for an R_RDY from the device.

The amount of **RX BB Credit** can be modified based upon which mode the port is operating in. If the port is operating as an F_Port, the **AdminFx** value can be modified. If the port is operating as an E_Port or TE_Port the **AdminISL** value can be modified. If you want to globally change the value regardless of which mode the port is operating in then the **Admin** value can be modified.

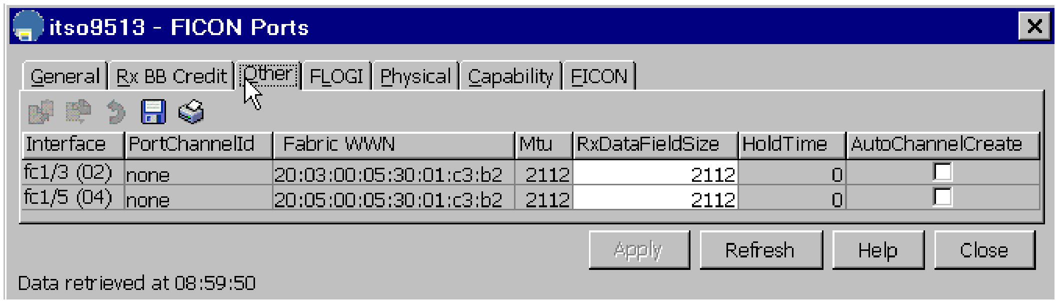

itso9513 - FICON Ports
General
Rx BB Credit
Other
FLOGI
Physical
Capability
FICON
Apply
Refresh
Help
Close

Interface	Oper	Model	Admin	Extended	AdminISL	AdminFx	PerfBuffer Admin	PerfBuffer Oper	Current Rx	Current Tx	BbScn Notify
fc1/3 (02)	16	regular	0	0	0	0	0	n/a	16	200	☑
fc1/5 (04)	16	regular	0	0	0	0	0	n/a	16	200	☑

Data retrieved at 08:59:37

Figure 4-204 DM display of FICON BB credit information

Figure 4-205 below provides the **Mtu** and **Wwn** (Fabric World Wide Name (fWWN) information for each interface). The Fabric WWN is the wwn of the switch port itself.

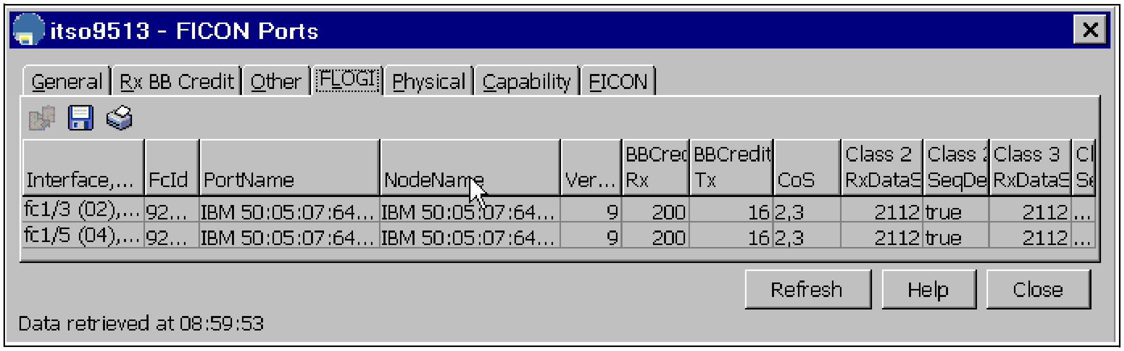

itso9513 - FICON Ports
General
Rx BB Credit
Other
FLOGI
Physical
Capability
FICON
Apply
Refresh
Help
Close

Interface	PortChannelId	Fabric WWN	Mtu	RxDataFieldSize	HoldTime	AutoChannelCreate
fc1/3 (02)	none	20:03:00:05:30:01:c3:b2	2112	2112	0	☐
fc1/5 (04)	none	20:05:00:05:30:01:c3:b2	2112	2112	0	☐

Data retrieved at 08:59:50

Figure 4-205 DM display FICON port information

Figure 4-206 shows the FICON specific **FLOGI** information for just this switch.This includes the negotiated buffer to buffer credits and class of service capability.

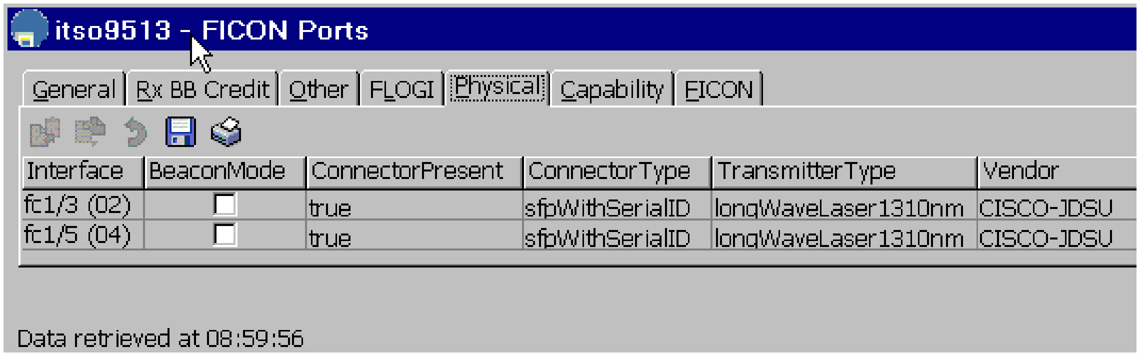

itso9513 - FICON Ports
General
Rx BB Credit
Other
FLOGI
Physical
Capability
FICON
Refresh
Help
Close

Interface,...	FcId	PortName	NodeName	Ver...	BBCred Rx	BBCredit Tx	CoS	Class 2 RxDataS	Class : SeqDe	Class 3 RxDataS	Cl Se
fc1/3 (02),...	92...	IBM 50:05:07:64...	IBM 50:05:07:64...	9	200	16	2,3	2112	true	2112	...
fc1/5 (04),...	92...	IBM 50:05:07:64...	IBM 50:05:07:64...	9	200	16	2,3	2112	true	2112	...

Data retrieved at 08:59:53

Figure 4-206 DM display of FICON FLOGI database for the 9506

Figure 4-207 displays the physical information such as what type of **Transmitter Type** (SFP) is present in the interface.

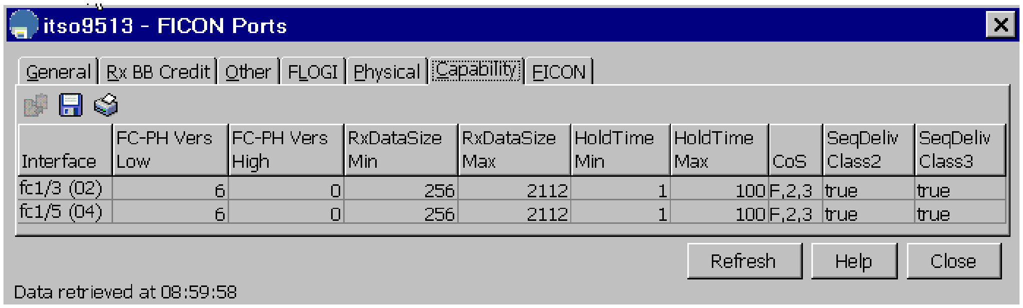

itso9513 - FICON Ports
General
Rx BB Credit
Other
FLOGI
Physical
Capability
FICON

Interface	BeaconMode	ConnectorPresent	ConnectorType	TransmitterType	Vendor
fc1/3 (02)	☐	true	sfpWithSerialID	longWaveLaser1310nm	CISCO-JDSU
fc1/5 (04)	☐	true	sfpWithSerialID	longWaveLaser1310nm	CISCO-JDSU

Data retrieved at 08:59:56

Figure 4-207 DM display of physical port attributes for the FICON ports

Figure 4-208 indicates the Fibre Channel attributes the switch port is capable of supporting. For example, from this display we can discern that the switch can support either class F, 2, or 3 types of service for connections to this port.

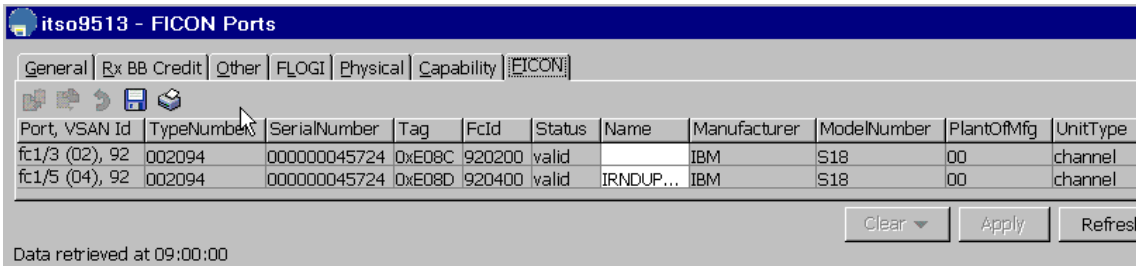

itso9513 - FICON Ports
General
Rx BB Credit
Other
FLOGI
Physical
Capability
FICON
Refresh
Help
Close

Interface	FC-PH Vers Low	FC-PH Vers High	RxDataSize Min	RxDataSize Max	HoldTime Min	HoldTime Max	CoS	SeqDeliv Class2	SeqDeliv Class3
fc1/3 (02)	6	0	256	2112	1	100	F,2,3	true	true
fc1/5 (04)	6	0	256	2112	1	100	F,2,3	true	true

Data retrieved at 08:59:58

Figure 4-208 DM display of capability for the FICON ports

Figure 4-209 displays the Request Node Identification Data (RNID) for the attached device.


itso9513 - FICON Ports
General
Rx BB Credit
Other
FLOGI
Physical
Capability
FICON
Clear
Apply
Refresh

Port, VSAN Id	TypeNumber	SerialNumber	Tag	FcId	Status	Name	Manufacturer	ModelNumber	PlantOfMfg	UnitType
fc1/3 (02), 92	002094	000000045724	0xE08C	920200	valid		IBM	S18	00	channel
fc1/5 (04), 92	002094	000000045724	0xE08D	920400	valid	IRNDUP...	IBM	S18	00	channel

Data retrieved at 09:00:00

Figure 4-209 DM display of FICON RNID information

Figure 4-210 shows the path in DM to look at the global name server which we display next.

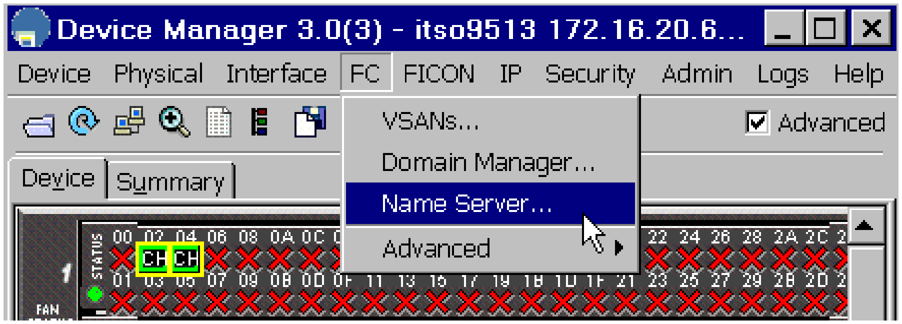
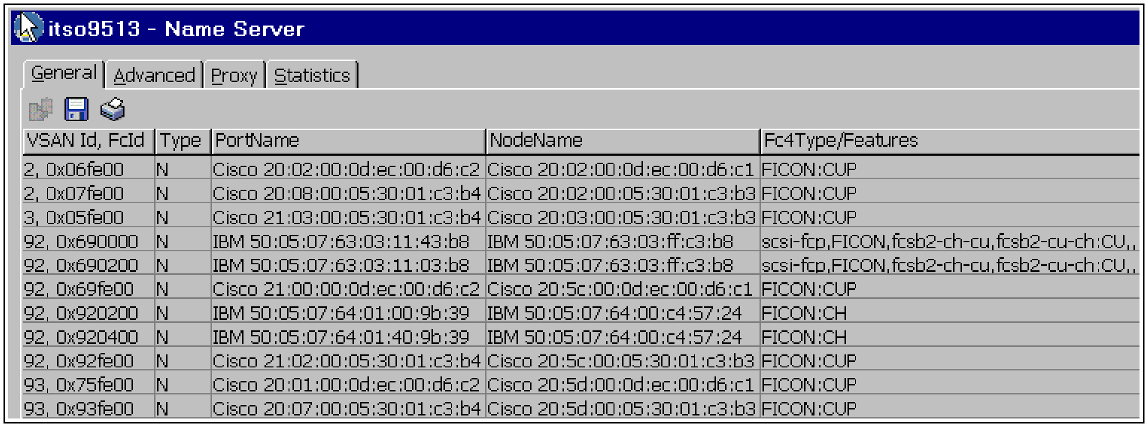

Device Manager 3.0(3) - itso9513 172.16.20.6...
Device
Physical
Interface
FC
FICON
IP
Security
Admin
Logs
Help
VSANs...
Domain Manager...
Name Server...
Advanced
☑ Advanced
Device
Summary
STATUS
FAN
CH
CH

Figure 4-210 Path to DM display of name server information

Figure 4-211 shows the global name server information. There are several interesting pieces of information in this display. For example, notice that the devices with **FcID** 0x690000 and 0x690200 have registered for both FICON (fcsb2) and Open Systems (scsi-fcp) support in the **FC4Type/Features** column.



VSAN Id, FcId	Type	PortName	NodeName	Fc4Type/Features
2, 0x06fe00	N	Cisco 20:02:00:0d:ec:00:d6:c2	Cisco 20:02:00:0d:ec:00:d6:c1	FICON:CUP
2, 0x07fe00	N	Cisco 20:08:00:05:30:01:c3:b4	Cisco 20:02:00:05:30:01:c3:b3	FICON:CUP
3, 0x05fe00	N	Cisco 21:03:00:05:30:01:c3:b4	Cisco 20:03:00:05:30:01:c3:b3	FICON:CUP
92, 0x690000	N	IBM 50:05:07:63:03:11:43:b8	IBM 50:05:07:63:03:ff:c3:b8	scsi-fcp,FICON,fcsb2-ch-cu,fcsb2-cu-ch:CU,,
92, 0x690200	N	IBM 50:05:07:63:03:11:03:b8	IBM 50:05:07:63:03:ff:c3:b8	scsi-fcp,FICON,fcsb2-ch-cu,fcsb2-cu-ch:CU,,
92, 0x69fe00	N	Cisco 21:00:00:0d:ec:00:d6:c2	Cisco 20:5c:00:0d:ec:00:d6:c1	FICON:CUP
92, 0x920200	N	IBM 50:05:07:64:01:00:9b:39	IBM 50:05:07:64:00:c4:57:24	FICON:CH
92, 0x920400	N	IBM 50:05:07:64:01:40:9b:39	IBM 50:05:07:64:00:c4:57:24	FICON:CH
92, 0x92fe00	N	Cisco 21:02:00:05:30:01:c3:b4	Cisco 20:5c:00:05:30:01:c3:b3	FICON:CUP
93, 0x75fe00	N	Cisco 20:01:00:0d:ec:00:d6:c2	Cisco 20:5d:00:0d:ec:00:d6:c1	FICON:CUP
93, 0x93fe00	N	Cisco 20:07:00:05:30:01:c3:b4	Cisco 20:5d:00:05:30:01:c3:b3	FICON:CUP

Figure 4-211 DM display of name server information

4.20 FICON configuration files

When the FICON feature on a VSAN is enabled, a file called an IPL file is automatically created with a default configuration. The IPL file contains port configuration information about each FICON port with regards to what other FICON ports are allowed to communicate with this port (prohibit function), whether this port is completely isolated from other FICON ports (block function), and the description or name of this FICON port.

This information is not stored in the startup-config or running-config of the switch as other configuration information is. This file was designed to specifically work with the CUP feature, but it can also be managed from both the CLI, as well as from FM and DM as shown in Figure 4-212.

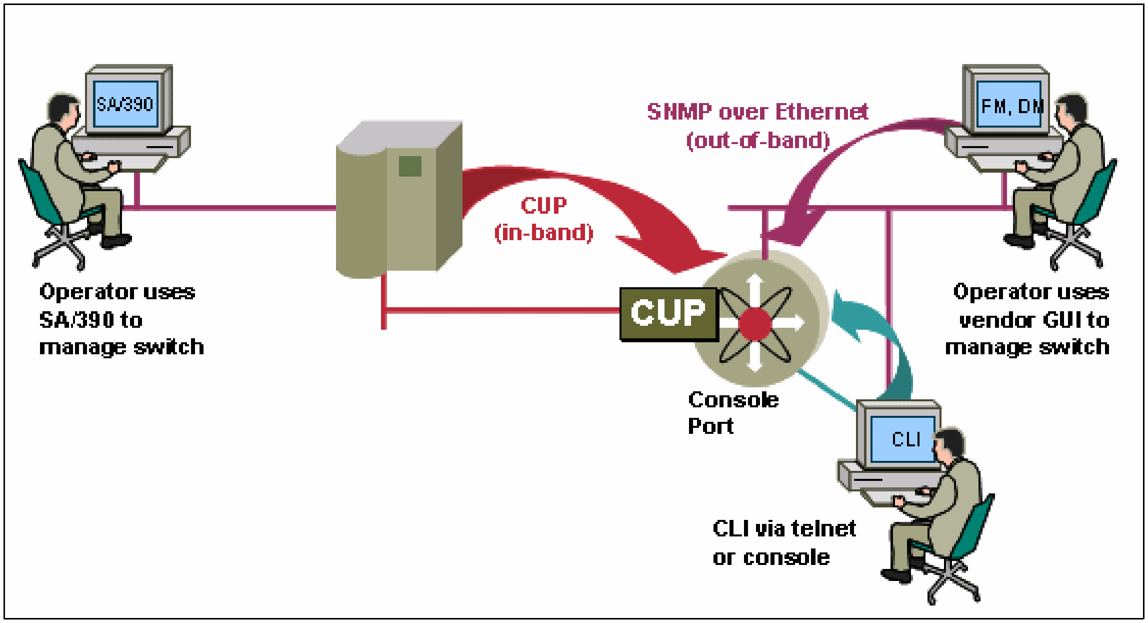

SA/390
SNMP over Ethernet
(out-of-band)
FM, DM
CUP
(in-band)
Operator uses
SA/390 to
manage switch
CUP
Operator uses
vendor GUI to
manage switch
Console
Port
CLI
CLI via telnet
or console

Figure 4-212 Managing FICON configuration files

You can save up to 16 FICON configuration files on each FICON VSAN. The files are in EBCDIC format and are saved in persistent storage, so they can survive a reload of the switch. FICON configuration files are maintained for each FICON VSAN and the names only have to be unique per FICON VSAN instance. For example, you can have a configuration file called ‘test’ for both FICON VSAN 5 and 10.

In addition to the port configuration attributes we described earlier, the following additional information is also stored in the FICON configuration file:

- Configure automatic saving of the FICON configuration
- FICON configuration for codepage on this VSAN
- Configuration of the last-byte of the FCID
- Enable host SA/390 control of the FICON VSAN
- Enable SNMP (FM/DM) control of this FICON VSAN.

These additional configuration settings can be viewed and modified using FM by opening the FICON VSAN that you want to view or modify, and select FICON from the list as shown in Figure 4-213.

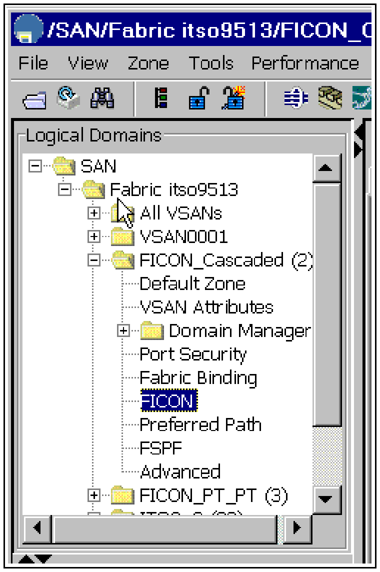
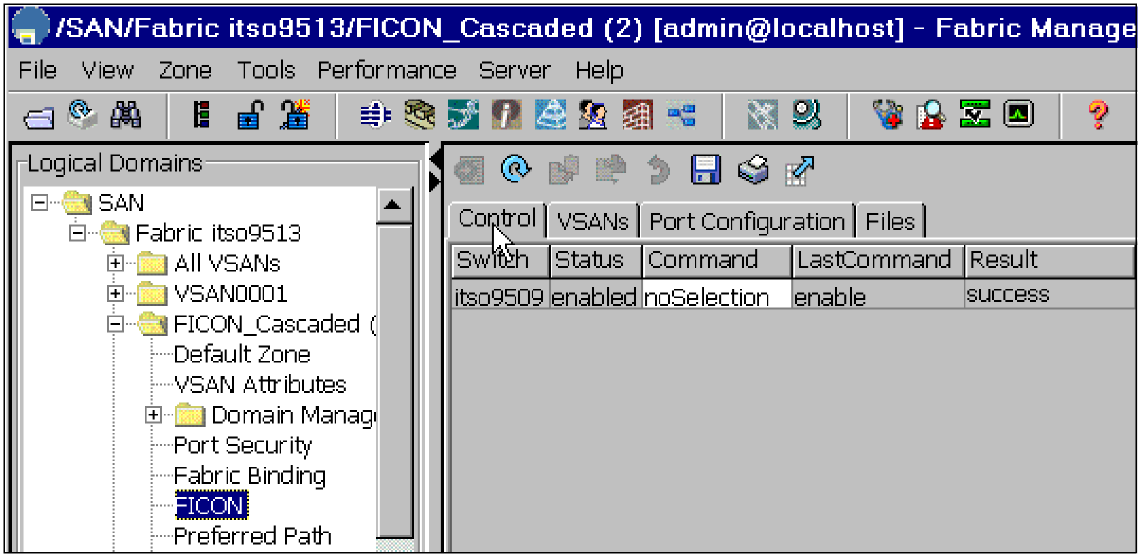

/SAN/Fabric itso9513/FICON_C
File View Zone Tools Performance
Logical Domains
SAN
Fabric itso9513
All VSANs
VSAN0001
FICON_Cascaded (2)
Default Zone
VSAN Attributes
Domain Manager
Port Security
Fabric Binding
FICON
Preferred Path
FSPF
Advanced
FICON_PT_PT (3)

Figure 4-213 Viewing FICON IPL file

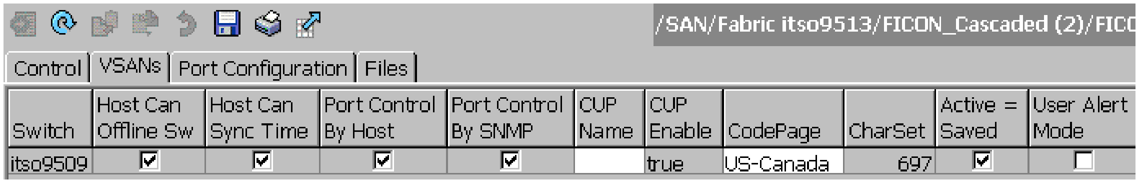
There are four tabs available. The first we show is the **Control** tab. This displays the information as shown in Figure 4-214.


/SAN/Fabric itso9513/FICON_Cascaded (2) [admin@localhost] - Fabric Manage
File View Zone Tools Performance Server Help
Logical Domains
SAN
Fabric itso9513
All VSANs
VSAN0001
FICON_Cascaded (
Default Zone
VSAN Attributes
Domain Manag
Port Security
Fabric Binding
FICON
Preferred Path
Control
VSANs
Port Configuration
Files

Switch	Status	Command	LastCommand	Result
itso9509	enabled	noSelection	enable	success

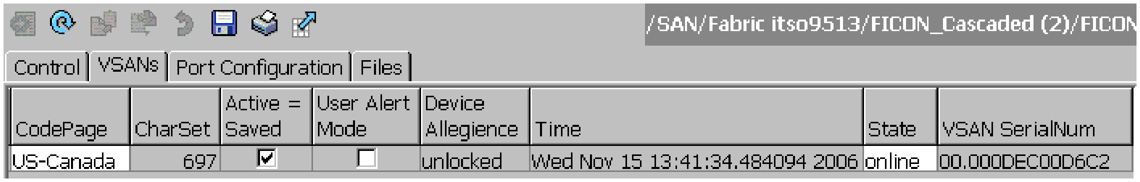
Figure 4-214 Control tab

In Figure 4-215 and Figure 4-216 we show the parameters on the **VSAN** tab.



Switch	Host Can Offline Sw	Host Can Sync Time	Port Control By Host	Port Control By SNMP	CUP Name	CUP Enable	CodePage	CharSet	Active = Saved	User Alert Mode
itso9509	☑	☑	☑	☑		true	US-Canada	697	☑	☐

Figure 4-215 VSAN attributes



CodePage	CharSet	Active = Saved	User Alert Mode	Device Allegience	Time	State	VSAN SerialNum
US-Canada	697	☑	☐	unlocked	Wed Nov 15 13:41:34.484094 2006	online	00.000DEC00D6C2

Figure 4-216 VSAN attributes continued

You can toggle any of the above IPL file attributes on or off, and then select the **Apply Changes** icon. The changes are then made to the active configuration. These changes are also saved into the IPL file immediately based upon the default **Active=Saved** feature. If this feature is off, changes are written *only* when you copy the switch's' running configuration to the startup configuration. All other FICON configuration information that is not contained in the IPL file is saved only after the running configuration has been copied to the startup configuration.

If **Port Control By Host** is enabled, then the SA/390 administrator can block, prohibit, or name ports. If not, then the port configuration can be viewed, but not modified.

If **Host Can Offline Switch** is enabled, then the SA/390 administrator user can take the VSAN offline and cause all ports in this VSAN to transmit the OLS primitive sequence.

If **Host Can Sync Time** is enabled, then the SA/390 administrator can sync the host and switch time for troubleshooting purposes.

> **Tip:** Setting the switch timezone can be done with the CLI **`clock timezone`** configuration command.

The switch can also be configured, **Port Control By SNMP**, to permit or deny an SNMP (FM/DM) user from modifying IPL file attributes. If the SNMP checkbox is toggled off, an FM/DM user cannot change any port attributes or any other setting that is stored in the FICON config files. FM/DM users could still view the status of the FICON VSAN.

> **Note:** After the SNMP box is unchecked, it can only be re-enabled via the CLI.

Device Allegiance refers to the mechanism whereby the IPL file is locked in order to avoid concurrent updates from multiple sources. Remember this file can be modified via SNMP, SA/390, and the CLI. This panel indicates if the file is locked or unlocked, and if locked, which device has the lock.

The FICON **CodePage** can also be modified here if necessary.

4.20.1 Using DM to prohibit and block ports

As mentioned previously, SNMP (DM) can be used to manage FICON configuration files, and as such can be used to prohibit, block, and swap ports. Before you make any changes to the FICON IPL configuration file it is recommended that you first make a backup copy of this file. This can be done by selecting **FICON->**VSANs as shown in Figure 4-217.

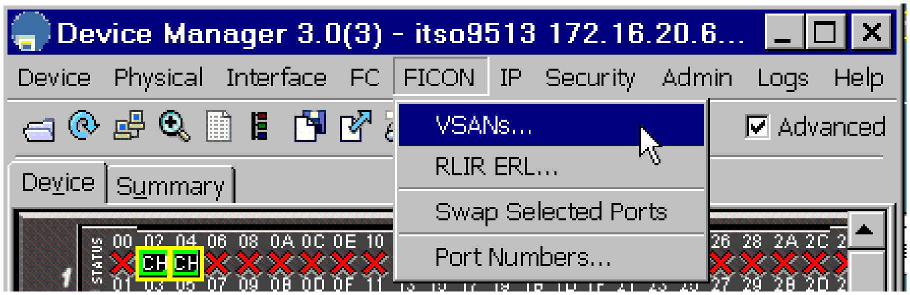
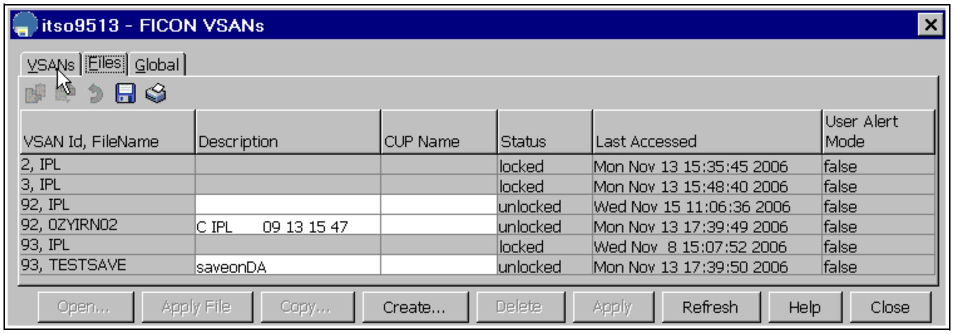

Device Manager 3.0(3) - itso9513 172.16.20.6...
Device
Physical
Interface
FC
FICON
IP
Security
Admin
Logs
Help
VSANs...
RLIR ERL...
Swap Selected Ports
Port Numbers...
☑ Advanced
Device
Summary
STATUS
CH
CH

Figure 4-217 Accessing FICON configuration files

Next select the **Files** tab as shown in Figure 4-218.

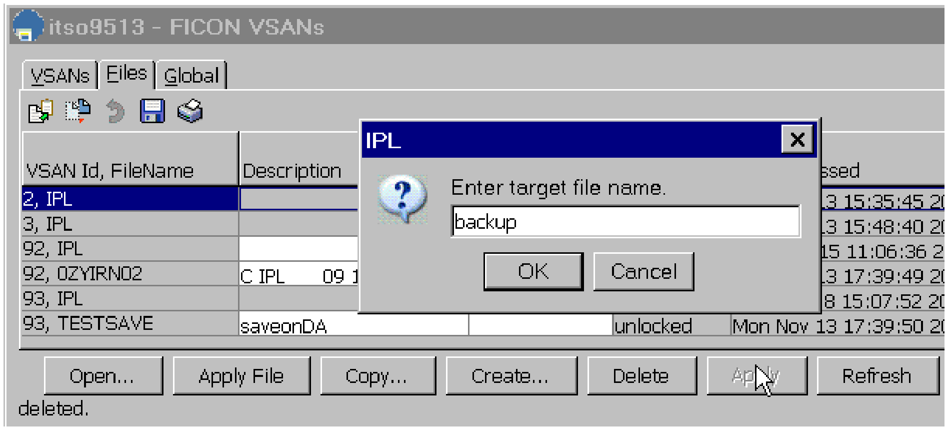

itso9513 - FICON VSANs
VSANs
Files
Global
Open...
Apply File
Copy...
Create...
Delete
Apply
Refresh
Help
Close

VSAN Id, FileName	Description	CUP Name	Status	Last Accessed	User Alert Mode
2, IPL			locked	Mon Nov 13 15:35:45 2006	false
3, IPL			locked	Mon Nov 13 15:48:40 2006	false
92, IPL			unlocked	Wed Nov 15 11:06:36 2006	false
92, 0ZYIRN02	C IPL 09 13 15 47		unlocked	Mon Nov 13 17:39:49 2006	false
93, IPL			locked	Wed Nov 8 15:07:52 2006	false
93, TESTSAVE	saveonDA		unlocked	Mon Nov 13 17:39:50 2006	false

Figure 4-218 Accessing FICON configuration files panel 2

At this point we *might* only see one configuration file, the IPL file, and if the **Active=Saved** feature is enabled, this file will be locked and it cannot be opened.

To make a copy of this file for backup purposes, click the IPL file you want to copy, select **Copy**, enter the name of the new file, and select **OK** as shown in Figure 4-219.

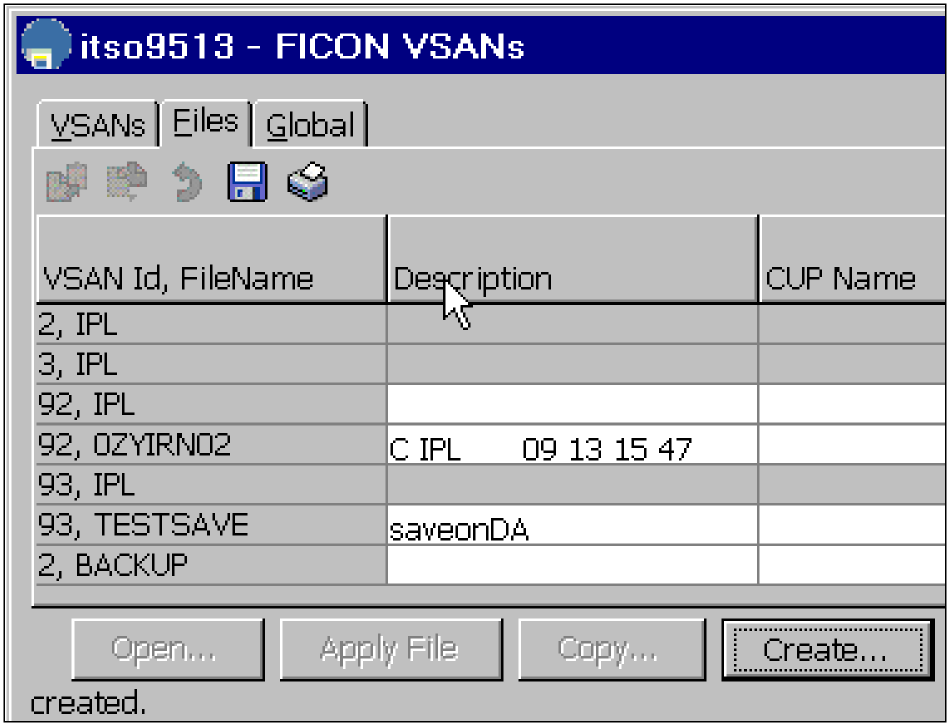

itso9513 - FICON VSANs
VSANs
Files
Global
VSAN Id, FileName
Description
2, IPL
3, IPL
92, IPL
92, 0ZYIRN02
93, IPL
93, TESTSAVE
IPL
OK
Cancel
Open...
Apply File
Copy...
Create...
Delete
Apply
Refresh
deleted.

Enter target file name.

backup

Figure 4-219 Creating a copy of the IPL configuration file

This creates a new file called *backup*, which is shown in Figure 4-220.

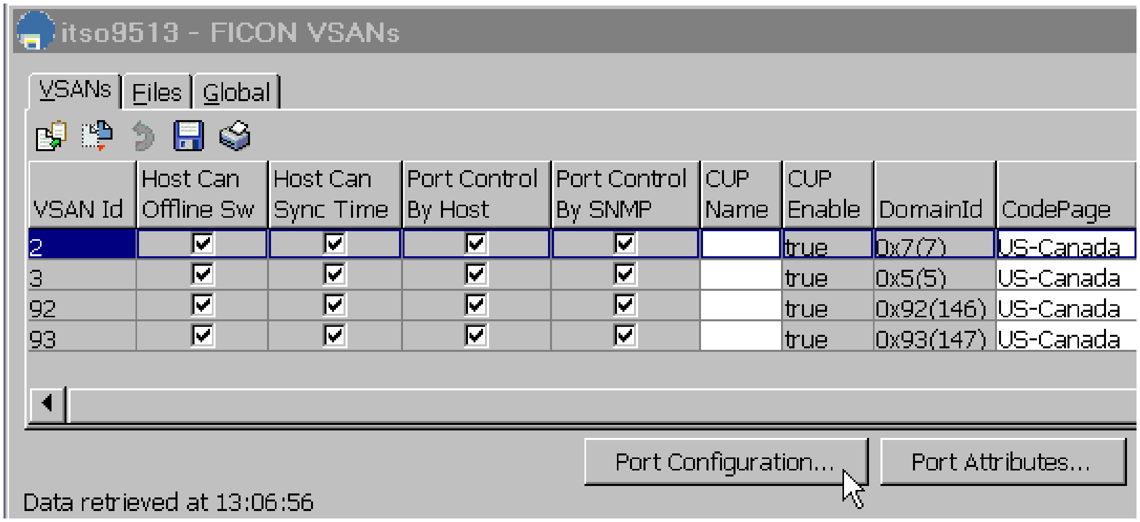

itso9513 - FICON VSANs
VSANs
Files
Global
Open...
Apply File
Copy...
Create...

VSAN Id, FileName	Description	CUP Name
2, IPL		
3, IPL		
92, IPL		
92, OZYIRN02	C IPL 09 13 15 47	
93, IPL		
93, TESTSAVE	saveonDA	
2, BACKUP		

created.

Figure 4-220 Newly created backup FICON configuration file

Now that a backup of the configuration file has been created (2, BACKUP), we can make changes directly to the IPL file by selecting the FICON VSAN we want to modify, and then by selecting **Port Configuration** as shown in Figure 4-221.

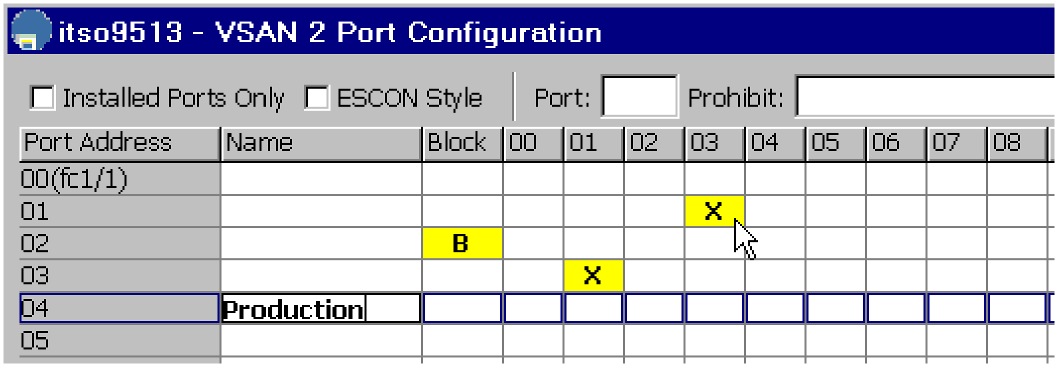

itso9513 - FICON VSANs
VSANs
Files
Global
Port Configuration...
Port Attributes...

VSAN Id	Host Can Offline Sw	Host Can Sync Time	Port Control By Host	Port Control By SNMP	CUP Name	CUP Enable	DomainId	CodePage
2	☑	☑	☑	☑		true	0x7(7)	US-Canada
3	☑	☑	☑	☑		true	0x5(5)	US-Canada
92	☑	☑	☑	☑		true	0x92(146)	US-Canada
93	☑	☑	☑	☑		true	0x93(147)	US-Canada

Data retrieved at 13:06:56

Figure 4-221 Modifying IPL port attributes

At this point, blocking and prohibiting ports is intuitive and can be accomplished by simply toggling on and off the column check boxes for the desired ports. In the example in Figure 4-222 we have blocked port 2 from all communication, prevented port 1 from communicating with port 3, and assigned the name 'Production' to port 4. Notice that if we move the cursor over a row and column, the intersecting port addresses are displayed (01/03), and when we click once in the port, a red **X** is entered and the corresponding row/port (03/01) is also automatically selected as well.

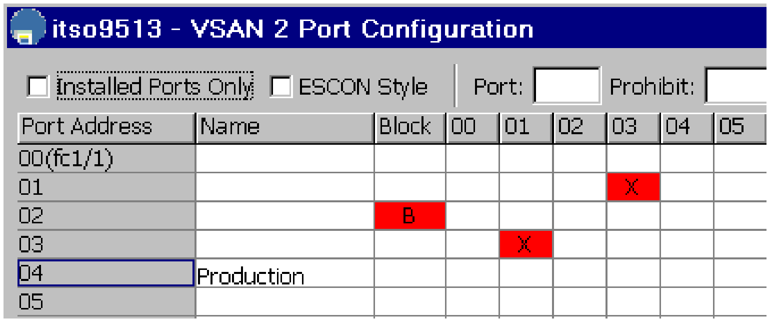

itso9513 - VSAN 2 Port Configuration
☐ Installed Ports Only
☐ ESCON Style
Port:
Prohibit:

Port Address	Name	Block	00	01	02	03	04	05	06	07	08
00(fc1/1)											
01						X					
02		B									
03				X							
04	Production										
05											

Figure 4-222 Prohibiting, blocking, and naming FICON ports

Tip: To view the available and prohibited ESCON style ports, check the ESCON Style box.

The only thing left to do at this point is **Apply** the changes. We can then verify our changes by reopening the **VSAN 2 Port Configuration** panel as shown in Figure 4-223.



Port Address	Name	Block	00	01	02	03	04	05
00(fc1/1)								
01						X		
02		B						
03				X				
04	Production							
05								

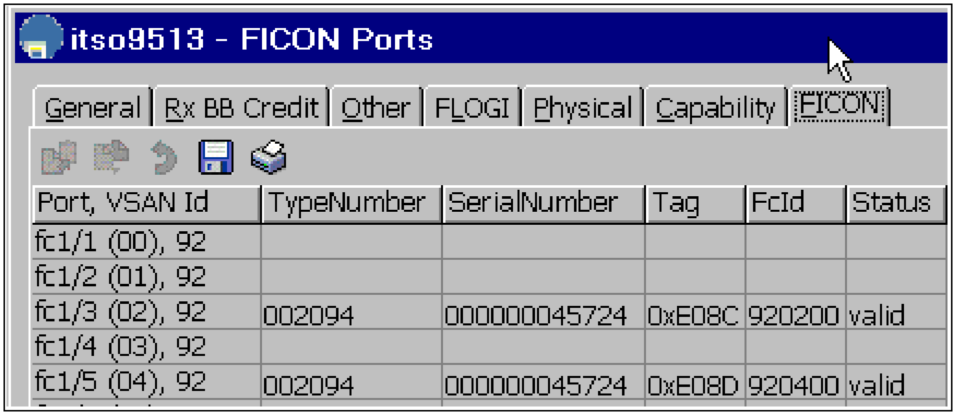
Figure 4-223 Verifying FICON port attribute changes

4.20.2 Using DM to swap ports

If there is a problem with a particular port, a feature called port swap can be used to move the FICON port address of one interface to a different FC interface that resides in the same switch. This temporarily circumvents the necessity to make HCD changes on the host.

Remember that the port number of FICON CUs is defined in the `LINK` parameter on the `CNTLUNIT` macro in IOCDS. Our goal is to swap the FICON port address for the CU on interface FC1/3 with interface FC1/5. Note that both the source and destination ports must be FICON ports, that is to say both ports must be members of the FICON VSAN.

First we verify the current port addresses of the interfaces. We do this by selecting **FICON** → **VSANs**, Now we click once on VSAN 92, and click **Port Attributes**, and then click the **FICON** tab as shown in Figure 4-224.


itso9513 - FICON Ports
General
Rx BB Credit
Other
FLOGI
Physical
Capability
FICON

Port, VSAN Id	TypeNumber	SerialNumber	Tag	FcId	Status
fc1/1 (00), 92					
fc1/2 (01), 92					
fc1/3 (02), 92	002094	000000045724	0xE08C	920200	valid
fc1/4 (03), 92					
fc1/5 (04), 92	002094	000000045724	0xE08D	920400	valid

Figure 4-224 Viewing FICON port attributes

Notice the FCIDs **920200** and **920400**.

At this point we have completed the physical cabling swap for interfaces fc1/3 and fc1/5 (ports 02 and 04 in our display) and we now port swap interfaces fc1/3 (02) with fc1/5(04) in DM by clicking once on fc1/3 (02), hold down the control key and click fc1/5(04), then select the **Swap Selected** Ports pull-down from the **FICON** toolbar menu option as shown in Figure 4-225.

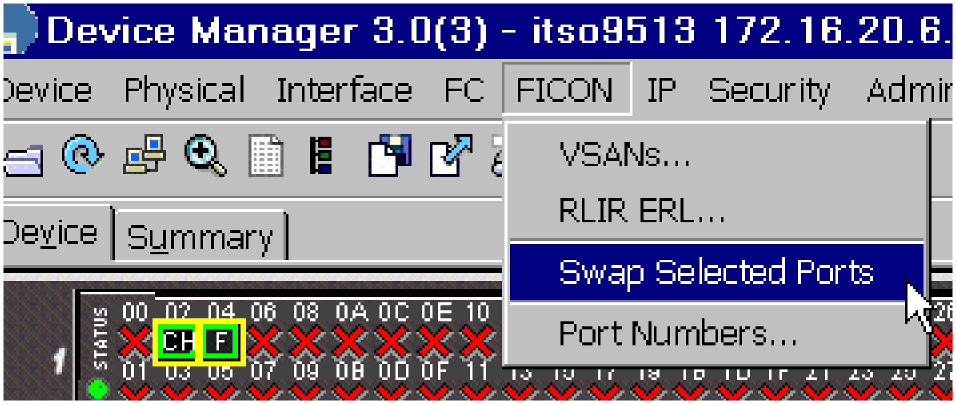
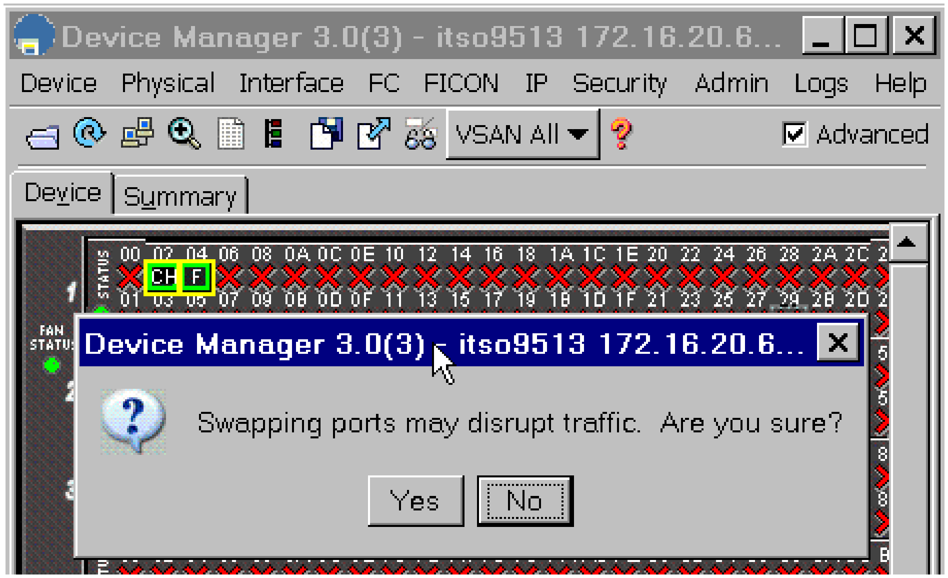

Device Manager 3.0(3) - itso9513 172.16.20.6.
Device
Physical
Interface
FC
FICON
IP
Security
Admir
VSANs...
RLIR ERL...
Swap Selected Ports
Port Numbers...
Device
Summary
STATUS
00 02 04 06 08 0A 0C 0E 10
CH
F
01 03 05 07 09 0B 0D 0F 11

Figure 4-225 Swapping selected ports

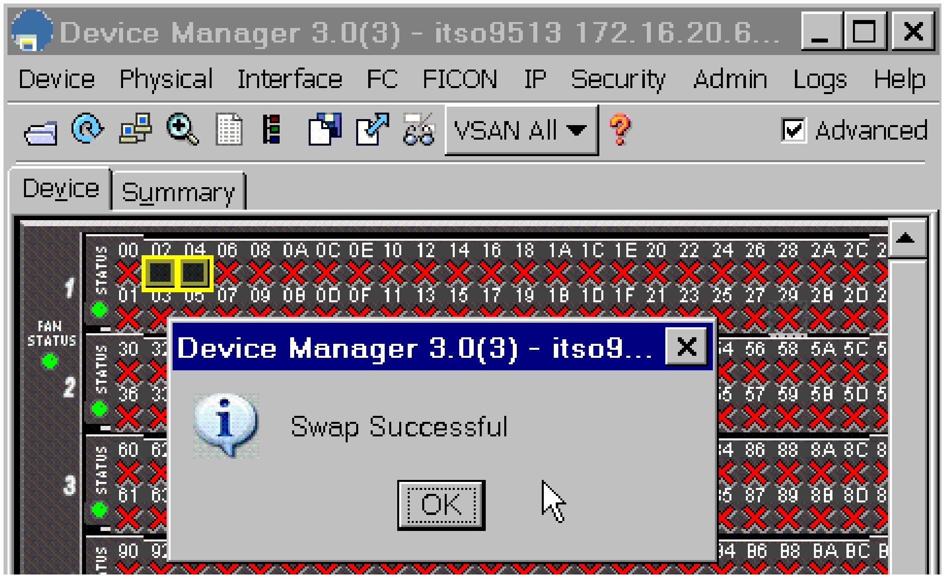
We are advised that this might be disruptive as shown in Figure 4-226.


Swapping ports may disrupt traffic. Are you sure?

Device Manager 3.0(3) - itso9513 172.16.20.6...
Device
Physical
Interface
FC
FICON
IP
Security
Admin
Logs
Help
VSAN All
☑ Advanced
Device
Summary
Device Manager 3.0(3) - itso9513 172.16.20.6...
Yes
No

Figure 4-226 Warning message

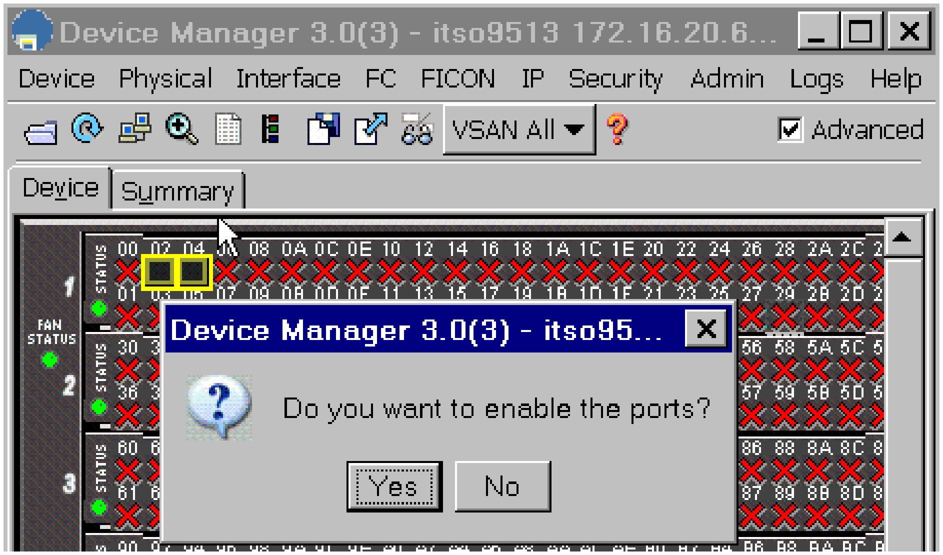
We see a message indicating that the swap was successful, as shown in Figure 4-227.


Device Manager 3.0(3) - itso9513 172.16.20.6...
Device Physical Interface FC FICON IP Security Admin Logs Help
VSAN All
Advanced
Device Summary
Device Manager 3.0(3) - itso9...
OK

Swap Successful

Figure 4-227 Port Swap successful message

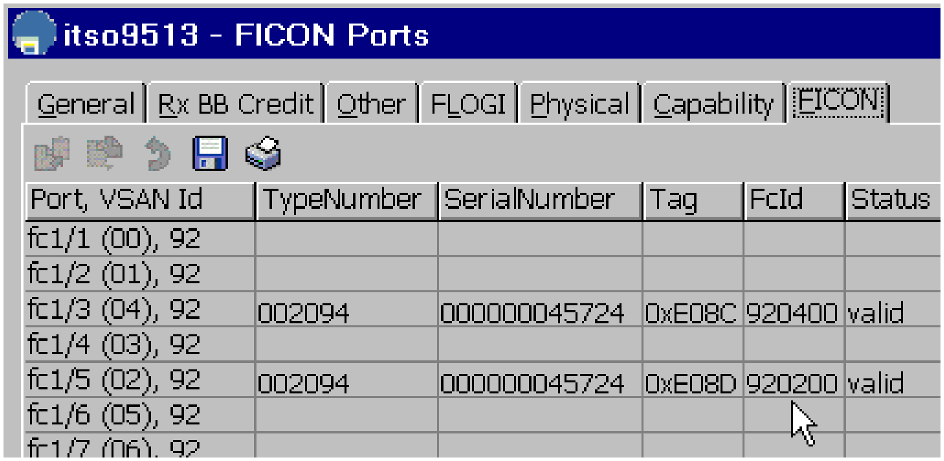
We are prompted to enable the ports as shown in Figure 4-228. We selected **Yes** because we have already moved the required cables.


Device Manager 3.0(3) - itso9513 172.16.20.6...
Device Physical Interface FC FICON IP Security Admin Logs Help
VSAN All
Advanced
Device Summary
Device Manager 3.0(3) - itso95...
Yes
No

Do you want to enable the ports?

Figure 4-228 Port Swap enable ports message

We can the verify that the port address was swapped, as shown in Figure 4-229, Notice how the FCIDs have changed when compared to Figure 4-224.


itso9513 - FICON Ports
General
Rx BB Credit
Other
FLOGI
Physical
Capability
FICON

Port, VSAN Id	TypeNumber	SerialNumber	Tag	FcId	Status
fc1/1 (00), 92					
fc1/2 (01), 92					
fc1/3 (04), 92	002094	000000045724	0xE08C	920400	valid
fc1/4 (03), 92					
fc1/5 (02), 92	002094	000000045724	0xE08D	920200	valid
fc1/6 (05), 92					
fc1/7 (06), 92					

Figure 4-229 FICON port attribute display after the port swap

This completes our FICON quickstart configuration topic.

Glossary

8b/10b A data encoding scheme developed by IBM, translating byte-wide data to an encoded 10-bit format. The Fibre Channel (FC) FC-1 level defines this as the method to use to encode and decode data transmissions over the Fibre Channel.

active configuration In an ESCON environment, the ESCON Director configuration determined by the status of the current set of connectivity attributes. Contrast with *saved configuration*.

adapter A hardware unit that aggregates other input/output (I/O) units, devices, or communications links to a system bus.

ADSM ADSTAR Distributed Storage Manager.

Advanced Intelligent Tape (AIT) A magnetic tape format by Sony that uses 8 mm cassettes, but is only used in specific drives.

agent In the client-server model, the part of the system that performs information preparation and exchange on behalf of a client or server application. In the Simple Network Management Protocol (SNMP), the managed system. See also *management agent*.

aggregation In the Storage Networking Industry Association Storage Model (SNIA), *virtualization* is known as *aggregation*. This aggregation can take place at the file level or at the level of individual blocks that are transferred to disk.

AIT See *Advanced Intelligent Tape*.

AL See *arbitrated loop*.

allowed In an ESCON Director, the attribute that, when set, establishes dynamic connectivity capability. Contrast with *prohibited*.

AL_PA Arbitrated Loop Physical Address.

American National Standards Institute (ANSI) The primary organization for fostering the development of technology standards in the United States. The ANSI family of Fibre Channel documents provides the standards basis for the Fibre Channel architecture and technology. See also *FC-PH*.

ANSI See *American National Standards Institute*.

APAR See *authorized program analysis report*.

arbitrated loop (AL) A Fibre Channel interconnection technology that allows up to 126 participating node ports and one participating fabric port to communicate.

arbitration The process of selecting one respondent from a collection of several candidates that request service concurrently.

Asynchronous Transfer Mode (ATM) A type of packet switching that transmits fixed-length units of data.

ATL See *Automated Tape Library*.

ATM See *Asynchronous Transfer Mode*.

authorized program analysis report (APAR) A report of a problem caused by a suspected defect in a current, unaltered release of a program.

Automated Tape Library (ATL) Large scale tape storage system, which uses multiple tape drives and mechanisms to address 50 or more cassettes.

backup A copy of computer data, or the act of copying such data, that is used to recreate data that has been lost, mislaid, corrupted, or erased.

bandwidth A measure of the information capacity of a transmission channel.

© Copyright IBM Corp. 1999-2007. All rights reserved.

basic mode An S/390® or IBM Eserver zSeries central processing mode that does not use logical partitioning. Contrast with *logically partitioned mode*.

blocked In an ESCON and FICON Director, the attribute that, when set, removes the communication capability of a specific port. Contrast with *unblocked*.

bridge A component used to attach more than one I/O unit to a port. Also a data communications device that connects two or more networks and forwards packets between them. The bridge may use similar or dissimilar media and signaling systems. It operates at the data link level of the OSI model. Bridges read and filter data packets and frames.

bridge/router A device that can provide the functions of a bridge, router, or both concurrently. A bridge/router can route one or more protocols, such as TCP/IP, and bridge all other traffic. See also *bridge* and *router*.

broadcast To send a transmission to all N_Ports on a fabric.

byte 1) In Fibre Channel, an eight-bit entity prior to encoding or after decoding, with its least significant bit denoted as bit 0 and most significant bit as bit 7. The most significant bit is shown on the left side in FC-FS unless otherwise shown. 2) In S/390 architecture or z/Architecture® for zSeries (and FICON), an eight-bit entity prior to encoding or after decoding, with its least significant bit denoted as bit 7 and most significant bit as bit 0. The most significant bit is shown on the left side in S/390 architecture and z/Architecture for zSeries.

cascaded switches The connecting of one Fibre Channel switch to another Fibre Channel switch, creating a cascaded switch route between two N_Nodes connected to a Fibre Channel fabric.

chained In an ESCON environment, pertaining to the physical attachment of two ESCON Directors (ESCDs) to each other.

channel 1) A processor system element that controls one channel path, whose mode of operation depends on the type of hardware to which it is attached. In a channel subsystem, each channel controls an I/O interface between the channel control element and the logically attached control units. 2) In ESA/390 or z/Architecture, the part of a channel subsystem that manages a single I/O interface between a channel subsystem and a set of controllers (control units).

channel to channel See *CTC*.

channel to converter See *CVC*.

channel-attached Devices attached directly by data channels (I/O channels) to a computer. Also refers to devices attached to a controlling unit by cables rather than by telecommunication lines.

channel I/O A form of I/O where request and response correlation is maintained through a form of source, destination, and request identification.

channel path (CHP) A single interface between a central processor and one or more control units along which signals and data can be sent to perform I/O requests.

channel path identifier (CHPID) In a channel subsystem, a value assigned to each installed channel path of the system that uniquely identifies that path to the system.

channel subsystem (CSS) Relieves the processor of direct I/O communication tasks, and performs path management functions. Uses a collection of subchannels to direct a channel to control the flow of information between I/O devices and main storage.

CHP See *channel path*.

CHPID See *channel path identifier*.

CIFS Common Internet File System.

cladding In an optical cable, the region of low refractive index surrounding the core. See also *core* and *optical fiber.*

Class of Service A Fibre Channel frame delivery scheme that exhibit a specified set of delivery characteristics and attributes.

Class-1 A class of service that provides dedicated connection between two ports with confirmed delivery or notification of nondeliverability.

Class-2 A class of service that provides a frame switching service between two ports with confirmed delivery or notification of nondeliverability.

Class-3 A class of service that provides frame switching datagram service between two ports or a multicast service between a multicast originator and one or more multicast recipients.

Class-4 A class of service that provides a fractional bandwidth virtual circuit between two ports with confirmed delivery or notification of nondeliverability.

Class-6 A class of service that provides a multicast connection between a multicast originator and one or more multicast recipients with confirmed delivery or notification of nondeliverability.

client A software program used to contact and obtain data from a *server* software program on another computer, often across a great distance. Each *client* program is designed to work specifically with one or more kinds of server programs, and each server requires a specific kind of client program.

client/server The relationship between machines in a communications network. The client is the requesting machine, and the server is the supplying machine. Also used to describe the information management relationship between software components in a processing system.

cluster A type of parallel or distributed system that consists of a collection of interconnected whole computers and is used as a single, unified computing resource.

CNC A mnemonic for an ESCON channel used to communicate to an ESCON-capable device.

coaxial cable A transmission media (cable) used for high-speed transmission. It is called *coaxial* because it includes one physical channel that carries the signal surrounded (after a layer of insulation) by another concentric physical channel, both of which run along the same axis. The inner channel carries the signal and the outer channel serves as a ground.

configuration matrix In an ESCON environment or FICON, an array of connectivity attributes that appear as rows and columns on a display device and can be used to determine or change active and saved ESCON or FICON director configurations.

connected In an ESCON Director, the attribute that, when set, establishes a dedicated connection between two ESCON ports. Contrast with *disconnected.*

connection In an ESCON Director, an association established between two ports that provides a physical communication path between them.

connectivity attribute In an ESCON and FICON Director, the characteristic that determines a particular element of a port's status. See *allowed, prohibited, blocked, unblocked, as well as connected* and *disconnected*.

control unit A hardware unit that controls the reading, writing, or displaying of data at one or more I/O units.

controller A component that attaches to the system topology through a channel semantic protocol that includes some form of request/response identification.

core In an optical cable, the central region of an optical fiber through which light is transmitted and that has an index of refraction greater than the surrounding cladding material. See also *cladding* and *optical fiber*.

coupler In an ESCON environment, link hardware used to join optical fiber connectors of the same type. Contrast with *adapter*.

CRC See *Cyclic Redundancy Check*.

CSS See *channel subsystem*.

CTC Channel-to-channel. A mnemonic for an ESCON channel attached to another ESCON channel, where one of the two ESCON channels is defined as an ESCON CTC channel and the other ESCON channel is defined as a ESCON CNC channel. Also a mnemonic for a FICON channel supporting a CTC Control Unit function logically or physically connected to another FICON channel that also supports a CTC Control Unit function. FICON channels supporting the FICON CTC control unit function are defined as normal FICON native (FC) mode channels.

CVC A mnemonic for an ESCON channel attached to an IBM 9034 convertor. The 9034 converts ESCON CVC signals to parallel channel interface (OEMI) communication operating in block multiplex mode (Bus and Tag).

Cyclic Redundancy Check (CRC) An error-correcting code used in Fibre Channel.

DASD See *direct access storage device.*

DAT See *Digital Audio Tape*.

data sharing A SAN solution in which files on a storage device are shared between multiple hosts.

datagram Refers to the Class 3 Fibre Channel Service that allows data to be sent rapidly to multiple devices attached to the fabric, with no confirmation of delivery.

DDM See *disk drive module.*

dedicated connection In an ESCON Director, a connection between two ports that is not affected by information contained in the transmission frames. This connection, which restricts those ports from communicating with any other port, can be established or removed only as a result of actions performed by a host control program or at the ESCD console. Contrast with *dynamic connection*.

Note: The two links having a dedicated connection appear as one continuous link.

default Pertaining to an attribute, value, or option that is assumed when none is explicitly specified.

Dense Wavelength Division Multiplexing (DWDM) The concept of packing multiple signals tightly together in separate groups, and transmitting them simultaneously over a common carrier wave.

destination Any point or location, such as a node, station, or a particular terminal, to which information is to be sent. An example is a Fibre Channel fabric F_Port; when attached to a Fibre Channel N_port, communication to the N_port via the F_port is said to be to the F_Port destination identifier (D_ID).

device A mechanical, electrical, or electronic contrivance with a specific purpose.

device address 1) In ESA/390 architecture and z/Architecture for zSeries, the field of an ESCON device-level frame that selects a specific device on a control unit image. 2) In the FICON channel FC-SB-2 architecture, the device address field in an SB-2 header that is used to select a specific device on a control unit image.

device number 1) In ESA/390 and z/Architecture for zSeries, a four-hexadecimal character identifier (for example, 19A0) that you associate with a device to facilitate communication between the program and the host operator. 2) The device number that you associate with a subchannel that uniquely identifies an I/O device.

dB Decibel. A ratio measurement distinguishing the percentage of signal attenuation (loss) between the I/O power. Attenuation is expressed as dB/km.

Digital Audio Tape (DAT) A tape media technology designed for very high quality audio recording and data backup. DAT cartridges look like audio cassettes and are often used in mechanical auto-loaders. Typically, a DAT cartridge provides 2 GB of storage, but new DAT systems have much larger capacities.

Digital Linear Tape (DLT) A magnetic tape technology originally developed by Digital Equipment Corporation (DEC) and now sold by Quantum. DLT cartridges provide storage capacities from 10 GB to 35 GB.

direct access storage device (DASD) A mass storage medium on which a computer stores data. any online storage device: a disc, drive or CD-ROM.

disconnected In an ESCON Director, the attribute that, when set, removes a dedicated connection. Contrast with *connected*.

disk A mass storage medium on which a computer stores data.

disk drive module (DDM) A disk storage medium that you use for any host data that is stored within a disk subsystem.

disk mirroring A fault-tolerant technique that writes data simultaneously to two hard disks using the same hard disk controller.

disk pooling A SAN solution in which disk storage resources are pooled across multiple hosts rather than dedicated to a specific host.

distribution panel In an ESCON and FICON environment, a panel that provides a central location for the attachment of trunk and jumper cables and can be mounted in a rack, wiring closet, or on a wall.

DLT See *Digital Linear Tape*.

duplex Pertaining to communication in which data or control information can be sent and received at the same time, from the same node. Contrast with *half duplex.*

duplex connector In an ESCON environment, an optical fiber component that terminates both jumper cable fibers in one housing and provides physical keying for attachment to a duplex receptacle.

duplex receptacle In an ESCON environment, a fixed or stationary optical fiber component that provides a keyed attachment method for a duplex connector.

DWDM See *Dense Wavelength Division Multiplexing*.

dynamic connection In an ESCON Director, a connection between two ports, established or removed by the ESCD and that, when active, appears as one continuous link. The duration of the connection depends on the protocol defined for the frames transmitted through the ports and on the state of the ports. Contrast with *dedicated connection.*

dynamic connectivity In an ESCON Director, the capability that allows connections to be established and removed at any time.

Dynamic I/O Reconfiguration An S/390 and z/Architecture function that allows I/O configuration changes to be made nondisruptively to the current operating I/O configuration.

ECL See *Emitter Coupled Logic*.

ELS See *Extended Link Services.*

EMIF See *ESCON Multiple Image Facility.*

Emitter Coupled Logic (ECL) The type of transmitter used to drive copper media such as Twinax, Shielded Twisted Pair, or Coax.

enterprise network A geographically dispersed network under the auspices of one organization.

Enterprise Systems Architecture/390® (ESA/390) An IBM architecture for mainframe computers and peripherals. Processors that follow this architecture include the S/390 Server family of processors.

Enterprise System Connection (ESCON) 1) An ESA/390 computer peripheral interface. The I/O interface uses ESA/390 logical protocols over a serial interface that configures attached units to a communication fabric. 2) A set of IBM products and services that provide a dynamically connected environment within an enterprise.

entity In general, a real or existing object from the Latin ens, or being, which makes the distinction between an object's existence and its qualities. In programming, engineering and probably many other contexts, the word is used to identify units, whether concrete items or abstract ideas, that have no ready name or label.

E_Port Expansion Port. A port on a switch used to link multiple switches together into a Fibre Channel switch fabric.

ESA/390 See *Enterprise Systems Architecture/390*.

ESCD Enterprise Systems Connection (ESCON) Director.

ESCD console The ESCON Director display and keyboard device used to perform operator and service tasks at the ESCD.

ESCON See *Enterprise System Connection.*

ESCON channel A channel having an Enterprise Systems Connection channel-to-control-unit I/O interface that uses optical cables as a transmission medium. May operate in CBY, CNC, CTC or CVC mode. Contrast with *parallel channel.*

ESCON Director An I/O interface switch that provides the interconnection capability of multiple ESCON interfaces (or FICON Bridge (FCV) mode - 9032-5) in a distributed-star topology.

ESCON Multiple Image Facility (EMIF) In the ESA/390 architecture and z/Architecture for zSeries, a function that allows logical partitions (LPARs) to share an ESCON and FICON channel path (and other channel types) by providing each LPAR with its own channel-subsystem image.

exchange A group of sequences which share a unique identifier. All sequences within a given exchange use the same protocol. Frames from multiple sequences can be multiplexed to prevent a single exchange from consuming all the bandwidth. See also *sequence*.

Extended Link Services (ELS) Via a command request, solicits a destination port (N_Port or F_Port) to perform a function or service. Each ELS request consists of an Link Service (LS) command; the N_Port ELS commands are defined in the FC-FS architecture.

fabric Fibre Channel employs a fabric to connect devices. A fabric can be as simple as a single cable connecting two devices. The term is most often used to describe a more complex network using hubs, switches, and gateways.

Fabric Login (FLOGI) Used by an N_Port to determine if a fabric is present and, if so, to initiate a session with the fabric by exchanging service parameters with the fabric. Fabric Login is performed by an N_Port following link initialization and before communication with other N_Ports is attempted.

Fabric Shortest Path First (FSPF) An intelligent path selection and routing standard and is part of the Fibre Channel Protocol.

FC 1) A short form when referring to something that is part of the Fibre Channel standard. Used by the IBM I/O definition process when defining a FICON channel (using IOCP of HCD) that will be used in FICON native mode (using the FC-SB-2 communication protocol. See also *Fibre Channel*.

FC-0 Lowest level of the Fibre Channel Physical standard, covering the physical characteristics of the interface and media.

FC-1 Middle level of the Fibre Channel Physical standard, defining the 8b/10b encoding and decoding and transmission protocol.

FC-2 Highest level of the Fibre Channel Physical standard, defining the rules for signaling protocol and describing transfer of frame, sequence, and exchanges.

FC-3 The hierarchical level in the Fibre Channel standard that provides common services such as striping definition.

FC-4 The hierarchical level in the Fibre Channel standard that specifies the mapping of upper-layer protocols to levels below.

FCA See *Fibre Channel Association*.

FC-AL See *Fibre Channel Arbitrated Loop*.

FC-CT Fibre Channel Common Transport Protocol

FC-FG See *Fibre Channel Fabric Generic*.

FC-FP See *Fibre Channel HIPPI Framing Protocol*.

FC-FS See *Fibre Channel-Framing and Signaling*.

FC-GS See *Fibre Channel Generic Services*.

FCLC See *Fibre Channel Loop Association*.

FC-LE See *Fibre Channel Link Encapsulation*.

FCP See *Fibre Channel Protocol*.

FC-PH See *Fibre Channel Physical and Signaling*.

FC-PLDA Fibre Channel Private Loop Direct Attach. See *Private Loop Direct Attach*.

FCS See *Fibre Channel standard*.

FC-SB See *Fibre Channel Single Byte Command Code Set*.

FC Storage Director SAN Storage Director.

FC-SW See *Fibre Channel Switch Fabric*.

fiber See *optical fiber*.

Fibre Channel A technology for transmitting data between computer devices at a data rate of up to 4 Gbps. It is especially suited for connecting computer servers to shared storage devices and for interconnecting storage controllers and drives.

Fibre Channel Arbitrated Loop (FC-AL) A reference to the FC-AL standard, a shared gigabit media for up to 127 nodes, one of which may be attached to a switch fabric. See also *arbitrated loop*.

Fibre Channel Association (FCA) A Fibre Channel industry association that works to promote awareness and understanding of the Fibre Channel technology and its application, and provides a means for implementers to support the standards committee activities.

Fibre Channel Fabric Generic (FC-FG) A reference to the document (ANSI X3.289-1996) which defines the concepts, behavior, and characteristics of the Fibre Channel fabric along with suggested partitioning of the 24-bit address space to facilitate the routing of frames.

Fibre Channel-Framing and Signaling (FC-FS) The term used to describe the FC-FS architecture.

Fibre Channel Generic Services (FC-GS) A reference to the document (ANSI X3.289-1996) that describes a common transport protocol used to communicate with the server functions, a full X500-based directory service, mapping of the SNMP directly to the Fibre Channel, a time server, and an alias server.

Fibre Channel HIPPI Framing Protocol (FCFP) A reference to the document (ANSI X3.254-1994) that defines how the HIPPI framing protocol is transported via the Fibre Channel.

Fibre Channel Link Encapsulation (FC-LE) A reference to the document (ANSI X3.287-1996) which defines how IEEE 802.2 Logical Link Control (LLC) information is transported via the Fibre Channel.

Fibre Channel Loop Association (FCLC) An independent working group of the FCA focused on the marketing aspects of the Fibre Channel loop technology.

Fibre Channel Physical and Signaling (FC-PH) A reference to the ANSI X3.230 standard, that contains the definition of the three lower levels (FC-0, FC-1, and FC-2) of the Fibre Channel.

Fibre Channel Protocol (FCP) The mapping of SCSI-3 operations to Fibre Channel.

Fibre Channel Service Protocol (FSP) The common FC-4 level protocol for all services, transparent to the fabric type or topology.

Fibre Channel Single Byte Command Code Set (FC-SB) A reference to the document (ANSI X.271-1996) which defines how the ESCON command set protocol is transported using the Fibre Channel.

Fibre Channel standard (FCS) An ANSI standard for a computer peripheral interface. The I/O interface defines a protocol for communication over a serial interface that configures attached units to a communication fabric. The protocol has four layers. The lower of the four layers defines the physical media and interface, the upper of the four layers defines one or more Upper Layer Protocols (ULP), for example, FCP for SCSI command protocols and FC-SB-2 for FICON protocol supported by ESA/390 and z/Architecture. Refer to ANSI X3.230.1999x.

Fibre Channel Switch Fabric (FC-SW) A reference to the ANSI standard under development that further defines the fabric behavior described in FC-FG and defines the communications between different fabric elements required for those elements to coordinate their operations and management address assignment.

fiber optic cable See *optical cable.*

fiber optics The branch of optical technology concerned with the transmission of radiant power through fibers made of transparent materials such as glass, fused silica, and plastic.

Note: Telecommunication applications of fiber optics use optical fibers. Either a single discrete fiber or a non-spatially aligned fiber bundle can be used for each information channel. Such fibers are often called “optical fibers” to differentiate them from fibers used in non-communication applications.

FICON 1) An ESA/390 and zSeries computer peripheral interface. The I/O interface uses ESA/390 and zSeries FICON protocols (FC-FS and FC-SB-2) over a Fibre Channel serial interface that configures attached units to a FICON supported Fibre Channel communication fabric. 2) An FC4 proposed standard that defines an effective mechanism for the export of the SBCCS-2 (FC-SB-2) command protocol via Fibre Channels.

FICON channel A channel having a Fibre Channel connection (FICON) channel-to-control-unit I/O interface that uses optical cables as a transmission medium. May operate in either FC or FCV mode.

FICON Director A Fibre Channel switch that supports the ESCON-like “control unit port” (CUP function) that is assigned a 24-bit Fibre Channel port address to allow FC-SB-2 addressing of the CUP function to perform command and data transfer. (In the Fibre Channel world, it is a means of in-band management using a FC-4 ULP.)

field replaceable unit (FRU) An assembly that is replaced in its entirety when any one of its required components fails.

F_Node Fabric Node. A fabric attached node.

FLOGI See *Fabric Login*.

F_Port Fabric Port. A port used to attach a Node Port (N_Port) to a switch fabric.

frame A linear set of transmitted bits that define the basic transport unit. The frame is the most basic element of a message in Fibre Channel communications, consisting of a 24-byte header and zero to 2112 bytes of data. See also *sequence*.

FRU See *field replaceable unit*.

FSP See *Fibre Channel Service Protocol*.

FSPF See *Fabric Shortest Path First*.

full duplex A mode of communications allowing simultaneous transmission and reception of frames.

gateway A node on a network that interconnects two otherwise incompatible networks.

Gbps Gigabits per second. Also sometimes referred to as Gb/s. In computing terms, it is approximately 1 000 000 000 bits per second. Most precisely it is 1 073 741 824 (1024 x 1024 x 1024) bits per second.

GBps Gigabytes per second. Also sometimes referred to as GB/s. In computing terms, it is approximately 1 000 000 000 bytes per second. Most precisely it is 1 073 741 824 (1024 x 1024 x 1024) bytes per second.

GBIC See *Gigabit Interface Converter*.

Gigabit One billion bits or one thousand megabits.

Gigabit Interface Converter (GBIC) Industry standard transceivers for connection of Fibre Channel nodes to arbitrated loop hubs and fabric switches.

Gigabit Link Module (GLM) A generic Fibre Channel transceiver unit that integrates the key functions necessary for the installation of a Fibre channel media interface on most systems.

GLM See *Gigabit Link Module*.

G_Port Generic Port. A generic switch port that is either an F_Port or E_Port. The function is automatically determined during login.

half duplex In data communication, pertaining to transmission in only one direction at a time. Contrast with *duplex.*

hard disk drive Storage media within a storage server used to maintain information that the storage server requires. Also a mass storage medium for computers that is typically available as a fixed disk or a removable cartridge.

hardware The mechanical, magnetic, and electronic components of a system, such as computers, telephone switches, and terminals.

HBA Host bus adapter.

HCD Hardware configuration dialog.

HDA See *head and disk assembly.*

HDD See *hard disk drive.*

head and disk assembly (HDA) The portion of an HDD associated with the medium and the read/write head.

hierarchical storage management (HSM) A software and hardware system that moves files from disk to slower, less expensive storage media based on rules and observation of file activity. Modern HSM systems move files from magnetic disk to optical disk to magnetic tape.

High Performance Parallel Interface (HPPI) An ANSI standard that defines a channel that transfers data between CPUs and from a CPU to disk arrays and other peripherals.

HIPPI See *High Performance Parallel Interface*.

HMMP HyperMedia Management Protocol.

HMMS See *HyperMedia Management Schema*.

hop An Fibre Channel frame may travel from a switch to a director, a switch to a switch, or a director to a director, which in this case is one hop.

HSM See *Hierarchical Storage Management*.

hub A Fibre Channel device that connects nodes into a logical loop by using a physical star topology. Hubs will automatically recognize an active node and insert the node into the loop. A node that fails or is powered off is automatically removed from the loop.

hub topology See *loop topology.*

Hunt Group A set of associated N_Ports attached to a single node, assigned a special identifier that allows any frames containing this identifier to be routed to any available N_Port in the set.

HyperMedia Management Schema (HMMS) The definition of an implementation-independent, extensible, common data description/schema, that allows data from a variety of sources to be described and accessed in real time regardless of the source of the data. See also *WEBM* and *HMMP.*

ID See *identifier.*

identifier A unique name or address that identifies such items as programs, devices, or systems.

in-band signaling Signaling that is carried in the same channel as the information. Also referred to as in-band.

in-band virtualization An implementation in which the virtualization process takes place in the data path between servers and disk systems. The virtualization can be implemented as software running on servers or in dedicated engines.

information unit A unit of information defined by an FC-4 mapping. Information units are transferred as a Fibre Channel sequence.

initial program load (IPL) 1) The initialization procedure that causes an operating system to commence operation. 2) The process by which a configuration image is loaded into storage at the beginning of a work day or after a system malfunction. (3) The process of loading system programs and preparing a system to run jobs.

input/output (I/O) 1) Pertaining to a device whose parts can perform an input process and an output process at the same time. 2) Pertaining to a functional unit or channel involved in an input process, output process, or both, concurrently or not, and to the data involved in such a process. (3) Pertaining to input, output, or both.

input/output configuration data set (IOCDS) The data set in the S/390 and zSeries processor (in the support element) that contains an I/O configuration definition built by the I/O configuration program (IOCP).

input/output configuration program (IOCP) An S/390 program that defines to a system the channels, I/O devices, paths to the I/O devices, and the addresses of the I/O devices. The output is normally written to a S/390 or zSeries IOCDS.

interface 1) A shared boundary between two functional units, defined by functional characteristics, signal characteristics, or other characteristics as appropriate. The concept includes the specification of the connection of two devices having different functions. 2) Hardware, software, or both, that link systems, programs, or devices.

intermix A mode of service defined by Fibre Channel that reserves the full Fibre Channel bandwidth for a dedicated Class 1 connection, but allows connection-less Class 2 traffic to share the link if the bandwidth is available.

inter-switch link (ISL) An Fibre Channel connection between switches and directors.

I/O See *input/output.*

I/O configuration The collection of channel paths, control units, and I/O devices that attaches to the processor. This may also include channel switches (for example, an ESCON Director).

IOCDS See *input/output configuration data set.*

IOCP See *input/output configuration control program.*

IODF The data set that contains the S/390 or zSeries I/O configuration definition file produced during the definition of the S/390 or zSeries I/O configuration by HCD. Used as a source for IPL, IOCP, and Dynamic I/O Reconfiguration.

IP Internet Protocol

IPI Intelligent Peripheral Interface

IPL See *initial program load*.

ISL See *inter-switch link*.

isochronous transmission Data transmission which supports network-wide timing requirements. A typical application for isochronous transmission is a broadcast environment which needs information to be delivered at a predictable time.

JBOD Just a bunch of disks.

jukebox A device that holds multiple optical disks and one or more disk drives, and can swap disks in and out of the drive as needed.

jumper cable In an ESCON and FICON environment, an optical cable having two conductors that provide physical attachment between a channel and a distribution panel or an ESCON/FICON Director port or a control unit/device, between an ESCON/FICON Director port and a distribution panel or a control unit/device, or between a control unit/device and a distribution panel. Contrast with *trunk cable.*

LAN See *local area network*.

laser A device that produces optical radiation using a population inversion to provide *light amplification by stimulated emission of radiation* and (generally) an optical resonant cavity to provide positive feedback. Laser radiation can be highly coherent temporally, spatially, or both.

latency A measurement of the time it takes to send a frame between two locations.

LC Lucent Connector. A registered trademark of Lucent Technologies.

LCU See *logical control unit.*

LED See *light emitting diode*.

licensed internal code (LIC) Microcode that IBM does not sell as part of a machine, but instead, licenses it to the client. LIC is implemented in a part of storage that is not addressable by user programs. Some IBM products use it to implement functions as an alternate to hard-wire circuitry.

light emitting diode (LED) A semiconductor chip that gives off visible or infrared light when activated. Contrast with *laser*.

link 1) In an ESCON environment or FICON environment (Fibre Channel environment), the physical connection and transmission medium used between an optical transmitter and an optical receiver. A link consists of two conductors, one used for sending and the other for receiving, thereby providing a duplex communication path. 2) In an ESCON I/O interface, the physical connection and transmission medium used between a channel and a control unit, a channel and an ESCD, a control unit and an ESCD, or at times between two ESCDs. 3) In a FICON I/O interface, the physical connection and transmission medium used between a channel and a control unit, a channel and a FICON Director, a control unit and a Fibre Channel FICON Director, or at times between two Fibre Channels switches.

link address 1) On an ESCON interface, the portion of a source or destination address in a frame that ESCON uses to route a frame through an ESCON director. ESCON associates the link address with a specific switch port that is on the ESCON director. 2) On a FICON interface, the port address (1-byte link address), or domain and port address (2-byte link address) portion of a source (S_ID) or destination address (D_ID) in a Fibre Channel frame that the Fibre Channel switch uses to route a frame through a Fibre Channel switch or Fibre Channel switch fabric. See also *port address.*

Link_Control_Facility A termination card that handles the logical and physical control of the Fibre Channel link for each mode of use.

LIP See *loop initialization primitive sequence*.

local area network (LAN) A computer network located in a user's premises within a limited geographic area, usually not larger than a floor or small building. Transmissions within a LAN are mostly digital, carrying data among stations at rates usually above one Mbps.

logical control unit (LCU) A separately addressable control unit function within a physical control unit. Usually a physical control unit that supports several LCUs. For ESCON, the maximum number of LCUs that can be in a control unit (and addressed from the same ESCON fiber link) is 16. They are addressed from x'0' to x'F'. For FICON architecture, the maximum number of LCUs that can be in a control unit (and addressed from the same FICON fibre link) is 256. They are addressed from x'00' to x'FF'. For both ESCON and FICON, the actual number supported, and the LCU address value, is both processor- and control unit implementation-dependent.

logical partition (LPAR) A set of functions that create a programming environment that is defined by the ESA/390 architecture or z/Architecture for zSeries. The ESA/390 architecture or z/Architecture for zSeries uses the term LPAR when more than one LPAR is established on a processor. An LPAR is conceptually similar to a virtual machine environment except that the LPAR is a function of the processor. Also, LPAR does not depend on an operating system to create the virtual machine environment.

logical switch number (LSN) A two-digit number used by the IOCP to identify a specific ESCON or FICON Director. This number is separate from the director's "switch device number" and, for FICON, it is separate from the director's "Fibre Channel switch address".

logically partitioned mode A central processor mode, available on the configuration frame when using the PR/SM™ facility, that allows an operator to allocate processor hardware resources among LPARs. Contrast with *basic mode.*

login server An entity within the Fibre Channel fabric that receives and responds to login requests.

loop circuit A temporary point-to-point like path that allows bidirectional communications between loop-capable ports.

loop initialization primitive (LIP) sequence A special Fibre Channel sequence that is used to start loop initialization. Allows ports to establish their port addresses.

loop topology An interconnection structure in which each point has physical links to two neighbors resulting in a closed circuit. In a loop topology, the available bandwidth is shared.

LPAR See *logical partition*.

L_Port Loop Port. A node or fabric port capable of performing arbitrated loop functions and protocols. NL_Ports and FL_Ports are loop-capable ports.

LSN See *logical switch number*.

Lucent Connector (LC) A registered trademark of Lucent Technologies

LVD Low Voltage Differential.

management agent A process that exchanges a managed node's information with a management station.

managed node A computer, a storage system, a gateway, a media device such as a switch or hub, a control instrument, a software product such as an operating system or an accounting package, or a machine on a factory floor, such as a robot.

managed object A variable of a managed node. This variable contains one piece of information about the node. Each node can have several objects.

Management Information Block (MIB) A formal description of a set of network objects that can be managed using the SNMP. The format is defined as part of SNMP and is a hierarchical structure of information relevant to a specific device, defined in object-oriented terminology as a collection of objects, relations, and operations among objects.

management station A host system that runs the management software.

MAR See *Media Access Rules*.

Mbps Megabits per second. Also sometimes referred to as Mb/s. In computing terms, it is approximately 1 000 000 bits per second. Most precisely it is 1 048 576 (1024 x 1024) bits per second.

MBps Megabytes per second. Also sometimes referred to as MB/s. In computing terms, it is approximately 1 000 000 bytes per second. Most precisely it is 1 048 576 (1024 x 1024) bytes per second.

media Plural of medium. The physical environment through which transmission signals pass. Common media include copper and fiber optic cable.

Media Access Rules (MAR) Enable systems to self-configure themselves is a SAN environment.

Media Interface Adapter (MIA) Enables optic-based adapters to interface with copper-based devices, including adapters, hubs, and switches.

metadata server In Storage Tank™, servers that maintain information (metadata) about the data files and grant permission for application servers to communicate directly with disk systems.

meter Equal to 39.37 inches, or just slightly larger than a yard (36 inches)

MIA See *Media Interface Adapter*.

MIB See *Management Information Block*.

mirroring The process of writing data to two separate physical devices simultaneously.

MM Multi-Mode. See *Multi-Mode Fiber*.

MMF See *Multi-Mode Fiber*.

multicast Sending a copy of the same transmission from a single source device to multiple destination devices on a fabric. This includes sending to all N_Ports on a fabric (broadcast) or to only a subset of the N_Ports on a fabric (multicast).

Multi-Mode Fiber (MMF) In optical fiber technology, an optical fiber that is designed to carry multiple light rays or modes concurrently, each at a slightly different reflection angle within the optical core. Multi-Mode fiber transmission is used for relatively short distances because the modes tend to disperse over longer distances. See also *Single-Mode Fiber*.

multiplex The ability to intersperse data from multiple sources and destinations onto a single transmission medium. Refers to delivering a single transmission to multiple destination N_Ports.

name server Provides translation from a given node name to one or more associated N_Port identifiers.

NAS See *Network Attached Storage*.

ND See *node descriptor*.

NDMP Network Data Management Protocol

NED See *node-element descriptor.*

network An aggregation of interconnected nodes, workstations, file servers, and peripherals, with its own protocol that supports interaction.

Network Attached Storage (NAS) A term used to describe a technology where an integrated storage system is attached to a messaging network that uses common communications protocols, such as TCP/IP.

Network File System (NFS) A distributed file system in UNIX developed by Sun Microsystems. It allows a set of computers to cooperatively access each other's files in a transparent manner.

Network Management System (NMS) A system responsible for managing at least part of a network. NMSs communicate with agents to help keep track of network statistics and resources.

network topology Physical arrangement of nodes and interconnecting communications links in networks based on application requirements and geographical distribution of users.

NFS See *Network File System*.

NL_Port Node Loop Port. A node port that supports arbitrated loop devices.

NMS See *Network Management System*. A system responsible for managing at least part of a network. NMSs communicate with agents to help keep track of network statistics and resources.

node An entity with one or more N_Ports or NL_Ports.

node descriptor (ND) In an ESCON and FICON environment, a 32-byte field that describes a node, channel, ESCON Director or FICON Director port, or a control unit.

node-element descriptor (NED) In an ESCON and FICON environment, a 32-byte field that describes a node element, such as a disk (DASD) device.

non-blocking Indicates that the capabilities of a switch are such that the total number of available transmission paths is equal to the number of ports. Therefore, all ports can have simultaneous access through the switch.

Non-L_Port A Node or Fabric port that is not capable of performing the arbitrated loop functions and protocols. N_Ports and F_Ports are not loop-capable ports.

N_Port Node Port. A Fibre Channel-defined hardware entity at the end of a link which provides the mechanisms necessary to transport information units to or from another node.

N_Port Login (PLOGI) Allows two N_Ports to establish a session and exchange identities and service parameters. It is performed following completion of the FLOGI process and prior to the FC-4 level operations with the destination port. May be either explicit or implicit.

OEMI See *original equipment manufacturer information.*

open system A system whose characteristics comply with standards made available throughout the industry and that can be connected to other systems that comply with the same standards.

operation A term defined in FC-2 that refers to one of the Fibre Channel *building blocks* composed of one or more, possibly concurrent, exchanges.

optical cable A fiber, multiple fibers, or a fiber bundle in a structure built to meet optical, mechanical, and environmental specifications. See also *jumper cable*, *optical cable assembly*, and *trunk cable.*

optical cable assembly An optical cable that is connector-terminated. Generally, an optical cable that has been connector-terminated by a manufacturer and is ready for installation. See also *jumper cable* and *optical cable*.

optical fiber Any filament made of dialectic materials that guides light, regardless of its ability to send signals. See also *fiber optics* and *optical waveguide*.

optical fiber connector A hardware component that transfers optical power between two optical fibers or bundles and is designed to be repeatedly connected and disconnected.

optical waveguide A structure capable of guiding optical power. In optical communications, generally a fiber designed to transmit optical signals. See *optical fiber.*

ordered set A Fibre Channel term referring to four 10 -bit characters (a combination of data and special characters) providing low-level link functions, such as frame demarcation and signaling between two ends of a link.

original equipment manufacturer information (OEMI) A reference to an IBM guideline for a computer peripheral interface. More specifically, it refers to IBM S/360™ and S/370™ Channel to Control Unit OEMI. The interface uses ESA/390 logical protocols over an I/O interface that configures attached units in a multi-drop bus environment. This OEMI interface is also supported by the zSeries 900 processors.

originator A Fibre Channel term referring to the initiating device.

out-of-band signaling Signaling that is separated from the channel carrying the information. Also referred to as *out-of-band*.

out-of-band virtualization An alternative type of virtualization in which servers communicate directly with disk systems under control of a virtualization function that is not involved in the data transfer.

parallel channel A channel having a System/360™ and System/370™ channel-to-control-unit I/O interface that uses bus and tag cables as a transmission medium. Contrast with *ESCON channel*.

path In a channel or communication network, any route between any two nodes. For ESCON and FICON, this is the route between the channel and the control unit/device, or sometimes from the operating system control block for the device and the device itself.

path group The ESA/390 and zSeries architecture (z/Architecture) term for a set of channel paths that are defined to a controller as being associated with a single S/390 image. The channel paths are in a group state and are online to the host.

path-group identifier ESA/390 and z/Architecture term for the identifier that uniquely identifies a given LPAR. The path-group identifier is used in communication between the system image program and a device. The identifier associates the path group with one or more channel paths, defining these paths to the control unit as being associated with the same system image.

PCICC (IBM) PCI Cryptographic Coprocessor.

peripheral Any computer device that is not part of the essential computer (the processor, memory and data paths) but is situated relatively close by. A near synonym is I/O device.

petard A device that is small and sometimes explosive.

PLDA See *Private Loop Direct Attach*.

PLOGI See *N_Port Login*.

point-to-point topology An interconnection structure in which each point has physical links to only one neighbor resulting in a closed circuit. In point-to-point topology, the available bandwidth is dedicated.

policy-based management Management of data on the basis of business policies (for example, “all production database data must be backed up every day”), rather than technological considerations (for example, “all data stored on this disk system is protected by remote copy”).

port An access point for data entry or exit. A receptacle on a device to which a cable for another device is attached. See also *duplex receptacle*.

port address In an ESCON Director, an address used to specify port connectivity parameters and to assign link addresses for attached channels and control units. In a FICON director or Fibre Channel switch, it is the middle 8 bits of the full 24-bit Fibre Channel port address. This field is also referred to as the *area field* in the 24-bit Fibre Channel port address. See also *link address.*

port bypass circuit A circuit used in hubs and disk enclosures to automatically open or close the loop to add or remove nodes on the loop.

port card In an ESCON and FICON environment, a field-replaceable hardware component that provides the optomechanical attachment method for jumper cables and performs specific device-dependent logic functions.

port name In an ESCON or FICON Director, a user-defined symbolic name of 24 characters or less that identifies a particular port.

Private Loop Direct Attach (PLDA) A technical report which defines a subset of the relevant standards suitable for the operation of peripheral devices such as disks and tapes on a private loop.

Private NL_Port An NL_Port which does not attempt login with the fabric and only communicates with other NL Ports on the same loop.

processor complex A system configuration that consists of all the machines required for operation; for example, a processor unit, a processor controller, a system display, a service support display, and a power and coolant distribution unit.

program temporary fix (PTF) A temporary solution or bypass of a problem diagnosed by IBM in a current unaltered release of a program.

prohibited In an ESCON or FICON Director, the attribute that, when set, removes dynamic connectivity capability. Contrast with *allowed.*

protocol 1) A set of semantic and syntactic rules that determine the behavior of functional units in achieving communication. 2) In Fibre Channel, the meaning of, and sequencing rules for, requests and responses used for managing the switch or switch fabric, transferring data, and synchronizing states of Fibre Channel fabric components. 3) A specification for the format and relative timing of information exchanged between communicating parties.

PTF See *program temporary fix*.

Public NL_Port An NL_Port that attempts login with the fabric and can observe the rules of either public or private loop behavior. A public NL_Port may communicate with both private and public NL_Ports.

QoS See *Quality of Service*.

Quality of Service (QoS) A set of communications characteristics required by an application. Each QoS defines a specific transmission priority, level of route reliability, and security level.

Quick Loop A unique Fibre Channel topology that combines arbitrated loop and fabric topologies. It is an optional licensed product that allows arbitrated loops with private devices to be attached to a fabric.

RAID See *Redundant Array of Inexpensive or Independent Disks.*

RAID 0 Level 0 RAID support. Striping, no redundancy.

RAID 1 Level 1 RAID support. Mirroring, complete redundancy.

RAID 5 Level 5 RAID support. Striping with parity.

Redundant Array of Inexpensive or Independent Disks (RAID) A method of configuring multiple disk drives in a storage subsystem for high availability and high performance.

repeater A device that receives a signal on an electromagnetic or optical transmission medium, amplifies the signal, and then retransmits it along the next leg of the medium.

responder A Fibre Channel term referring to the answering device.

route The path that an ESCON frame takes from a channel through an ESCD to a control unit/device.

router 1) A device that can decide which of several paths network traffic will follow based on some optimal metric. Routers forward packets from one network to another based on network-layer information. 2) A dedicated computer hardware or software package which manages the connection between two or more networks. See also *bridge* and *bridge/router*.

SAF-TE SCSI Accessed Fault-Tolerant Enclosures.

SAN See *storage area network*.

SAN See *System Area Network*.

SANSymphony In-band block-level virtualization software made by DataCore Software Corporation and resold by IBM.

saved configuration In an ESCON or FICON Director environment, a stored set of connectivity attributes whose values determine a configuration that can be used to replace all or part of the ESCD's or FICON's active configuration. Contrast with *active configuration*.

SC connector A fiber optic connector standardized by ANSI TIA/EIA-568A for use in structured wiring installations.

scalability The ability of a computer application or product (hardware or software) to continue to function because of a change in size or volume. For example, the ability to retain performance levels when adding additional processors, memory, and storage.

SCSI See *Small Computer System Interface.*

SCSI-3 SCSI-3 consists of a set of primary commands and additional specialized command sets to meet the needs of specific device types. The SCSI-3 command sets are used not only for the SCSI-3 parallel interface but for additional parallel and serial protocols, including Fibre Channel, Serial Bus Protocol (used with IEEE 1394 Firewire physical protocol), and the Serial Storage Protocol (SSP).

SCSI Enclosure Services (SES) ANSI SCSI-3 proposal that defines a command set for soliciting basic device status (temperature, fan speed, power supply status, etc.) from a storage enclosures.

SCSI-FCP The term used to refer to the ANSI Fibre Channel Protocol for SCSI document (X3.269-199x) that describes the FC-4 protocol mappings and the definition of how the SCSI protocol and command set are transported using a Fibre Channel interface.

SE See *service element*.

sequence A series of frames strung together in numbered order which can be transmitted over a Fibre Channel connection as a single operation. See also *exchange*.

SERDES Serializer Deserializer.

Serial Storage Architecture (SSA) A high speed serial loop-based interface developed as a high speed point-to-point connection for peripherals, particularly high speed storage arrays, RAID, and CD-ROM storage by IBM.

server A computer which is dedicated to one task.

service element (SE) A dedicated service processing unit used to service a S/390 machine (processor).

SES See *SCSI Enclosure Services.*

Simple Network Management Protocol (SNMP) The Internet network management protocol that provides a means to monitor and set network configuration and run-time parameters.

Single-Mode Fiber (SMF) In optical fiber technology, an optical fiber that is designed for the transmission of a single ray or mode of light as a carrier. It is a single light path used for long-distance signal transmission. See also *Multi-Mode Fiber*.

Small Computer System Interface (SCSI) 1) A set of evolving ANSI standard electronic interfaces that allow personal computers to communicate with peripheral hardware such as disk drives, tape drives, CD_ROM drives, printers, and scanners faster and more flexibly than previous interfaces. The interface uses a SCSI logical protocol over an I/O interface that configures attached targets and initiators in a multidrop bus topology. The following table identifies the major characteristics of the different SCSI versions.

SCSI version	Signal rate (MHz)	BusWidth (bits)	Maximum DTR (MBps)	Maximum no. devices	Maximum cable length (m)
SCSI-1	5	8	5	7	6
SCSI-2	5	8	5	7	6
Wide SCSI-2	5	16	10	15	6
Fast SCSI-2	10	8	10	7	6
Fast Wide SCSI-2	10	16	20	15	6
Ultra™ SCSI	20	8	20	7	1.5
Ultra SCSI-2	20	16	40	7	12
Ultra2 LVD SCSI	40	16	80	15	12

SM Single Mode. See *Single-Mode Fiber*.

SMART Self Monitoring and Reporting Technology.

SMF See *Single-Mode Fiber*.

SNIA See *Storage Networking Industry Association*.

SN storage network. See also *SAN*.

SNMP See *Simple Network Management Protocol*.

SNMWG See *Storage Network Management Working Group.*

SSA See *Serial Storage Architecture.*

star The physical configuration used with hubs in which each user is connected by communications links radiating out of a central hub that handles all communications.

storage area network (SAN) A dedicated, centrally managed, secure information infrastructure, which enables any-to-any interconnection of servers and storage systems.

storage media The physical device onto which data is recorded. Magnetic tape, optical disks, and floppy disks are all storage media.

Storage Network Management Working Group (SNMWG) Chartered to identify, define, and support open standards needed to address the increased management requirements imposed by storage area network environments.

Storage Networking Industry Association (SNIA) A non-profit organization comprised of more than 77 companies and individuals in the storage industry.

Storage Tank An IBM file aggregation project that enables a pool of storage, and even individual files, to be shared by servers of different types. In this way, Storage Tank can greatly improve storage utilization and enables data sharing.

StorWatch Expert StorWatch applications that employ a three-tiered architecture that includes a management interface, a StorWatch manager and agents that run on the storage resource or resources being managed. Products employ a StorWatch database that can be used for saving key management data, such as capacity or performance metrics. Products also use the agents and analysis of storage data saved in the database to perform higher value functions including the reporting of capacity and performance over time (trends), configuration of multiple devices based on policies, monitoring of capacity and performance, automated responses to events or conditions, and storage related data mining.

StorWatch Specialist A StorWatch interface for managing an individual Fibre Channel device or a limited number of like devices (that can be viewed as a single group). Typically provide simple, point-in-time management functions such as configuration, reporting on asset and status information, simple device and event monitoring, and some service utilities.

STP Shielded Twisted Pair.

striping A method for achieving higher bandwidth using multiple N_Ports in parallel to transmit a single information unit across multiple levels.

subchannel A logical function of a channel subsystem associated with the management of a single device.

subsystem A secondary or subordinate system, or programming support, usually capable of operating independently of or asynchronously with a controlling system.

SWCH In ESCON Manager, the mnemonic used to represent an ESCON Director.

switch A component with multiple entry and exit points (ports) that provides dynamic connection between any two of these points.

switch topology An interconnection structure in which any entry point can be dynamically connected to any exit point. The available bandwidth is scalable.

system area network (SAN) Term originally used to describe a particular symmetric multiprocessing (SMP) architecture in which a switched interconnect is used in place of a shared bus. Server area network refers to a switched interconnect between multiple SMPs.

T11 A technical committee of the National Committee for Information Technology Standards, titled T11 I/O Interfaces. Develops standards for moving data into and out of computers.

tape backup Making magnetic tape copies of hard disk and optical disc files for disaster recovery.

tape pooling A SAN solution in which tape resources are pooled and shared across multiple hosts rather than being dedicated to a specific host.

TCP See *Transmission Control Protocol.*

TCP/IP See *Transmission Control Protocol/ Internet Protocol.*

time server A Fibre Channel-defined service function that allows for the management of all timers used within a Fibre Channel system.

topology An interconnection scheme that allows multiple Fibre Channel ports to communicate. For example, point-to-point, arbitrated loop, and switched fabric are all Fibre Channel topologies.

TL_Port A private to public bridging of switches or directors, referred to as Translative Loop.

T_Port An ISL port more commonly known as an E_Port, referred to as a Trunk port and used by INRANGE.

Transmission Control Protocol (TCP) A reliable, full duplex, connection-oriented end-to-end transport protocol running on top of IP.

Transmission Control Protocol/ Internet Protocol (TCP/IP) A set of communications protocols that support peer-to-peer connectivity functions for both LAN and WANs.

trunk cable In an ESCON and FICON environment, a cable consisting of multiple fiber pairs that do not directly attach to an active device. This cable usually exists between distribution panels (or sometimes between a set processor channels and a distribution panel) and can be located within, or external to, a building. Contrast with *jumper cable*.

twinax A transmission media (cable) consisting of two insulated central conducting leads of coaxial cable.

twisted pair The most common type of transmission media (cable), that consists of two insulated copper wires twisted around each other to reduce the induction (interference) from one wire to another. The twists, or lays, are varied in length to reduce the potential for signal interference between pairs. Several sets of twisted pair wires may be enclosed in a single cable.

ULP Upper Level Protocols,

unblocked In an ESCON and FICON Director, the attribute that, when set, establishes communication capability for a specific port. Contrast with *blocked.*

Under-The-Covers (UTC) A term used to characterize a subsystem in which a small number of hard drives are mounted inside a higher function unit. The power and cooling are obtained from the system unit. Connection is by parallel copper ribbon cable or pluggable backplane, using IDE or SCSI protocols.

unit address The ESA/390 and zSeries term for the address associated with a device on a given controller. On ESCON and FICON interfaces, the unit address is the same as the device address. On OEMI interfaces, the unit address specifies a controller and device pair on the interface.

UTC See *Under-The-Covers*.

UTP Unshielded Twisted Pair

virtual circuit A unidirectional path between two communicating N_Ports that permits fractional bandwidth.

virtualization An abstraction of storage where the representation of a storage unit to the operating system and applications on a server is divorced from the actual physical storage where the information is contained.

virtualization engine Dedicated hardware and software that are used to implement virtualization.

WAN See *wide area network*.

Wave Division Multiplexing (WDM) A technology that puts data from different sources together on an optical fiber, with each signal carried on its own separate light wavelength. Using WDM, up to 80 (and theoretically more) separate wavelengths or channels of data can be multiplexed into a stream of light transmitted on a single optical fiber.

WDM See *Wave Division Multiplexing*.

Web-Based Enterprise Management (WEBM) A consortium working on the development of a series of standards to enable active management and monitoring of network-based elements.

WEBM See *Web-Based Enterprise Management*.

wide area network (WAN) A network which encompasses inter-connectivity between devices over a wide geographic area. A WAN may be privately owned or rented, but the term usually indicates the inclusion of public (shared) networks.

z/Architecture An IBM architecture for mainframe computers and peripherals. Processors that follow this architecture include the zSeries family of processors.

zoning In Fibre Channel environments, the grouping together of multiple ports to form a virtual private storage network. Ports that are members of a group or zone can communicate with each other but are isolated from ports in other zones.

zSeries A family of IBM mainframe servers that support high performance, availability, connectivity, security, and integrity.

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this Redbooks publication.

Redbooks

- *Introduction to Storage Area Networks*, SG24-5470
- *IBM TotalStorage: SAN Product, Design, and Optimization Guide*, SG24-6384
- *SAN Multiprotocol Routing: An Introduction and Implementation*, SG24-7321
- *IBM Enterprise Storage Server*, SG24-5465
- *IBM Tape Solutions for Storage Area Networks and FICON*, SG24-5474
- *Implementing Linux with IBM Disk Storage*, SG24-6261
- *Introduction to SAN Distance Solutions*, SG24-6408
- *Introducing Hosts to the SAN Fabric*, SG24-6411
- *FICON Implementation Guide*, SG24-6497

© Copyright IBM Corp. 1999-2007. All rights reserved.

Other resources

These publications are also relevant as further information sources:

- Clark, Tom. *IP SANs: An Introduction to iSCSI, iFCP, and FCIP Protocols for Storage Area Network*. Addison-Wesley Professional, first edition, December 2001. ISBN 0201752778.
- Farley, Marc. *Building Storage Networks*. McGraw-Hill/Osborne Media, first edition, January 2000. ISBN 0072120509.
- Judd, Josh. *Multiprotocol Routing for SAN*s. Infinity Publishing, October 2004. ISBN 0741423065.

Referenced Web sites

These Web sites are also relevant as further information sources:

- IBM TotalStorage hardware, software, and solutions:

  `http://www.storage.ibm.com`
- IBM TotalStorage storage area network:

  `http://www.storage.ibm.com/snetwork/index.html`
- Brocade:

  `http://www.brocade.com`
- Cisco:

  `http://www.cisco.com`
- McDATA:

  `http://www.inrange.com/`
- QLogic:

  `http://www.qlogic.com`
- Emulex:

  `http://www.emulex.com`
- Finisar:

  `http://www.finisar.com`
- Veritas:

  `http://www.veritas.com`
- Tivoli:

  `http://www.tivoli.com`

- JNI:

  `http://www.Jni.com`
- IEEE:

  `http://www.ieee.org`
- Storage Networking Industry Association:

  `http://www.snia.org`
- SCSI Trade Association:

  `http://www.scsita.org`
- Internet Engineering Task Force:

  `http://www.ietf.org`
- American National Standards Institute:

  `http://www.ansi.org`
- Technical Committee T10:

  `http://www.t10.org`
- Technical Committee T11:

  `http://www.t11.org`
- xSeries 430 and NUMA-Q Information Center:

  `http://publib.boulder.ibm.com/xseries/`

How to get Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads:

ibm.com/support

IBM Global Services:

ibm.com/services

Index

Numerics
16-port blades 14
2005-B16 9, 13
2109-F16 License Administration 126
2109-M14 16, 39, 54
2109-M48 9, 14, 16
9020 726, 729, 733
9120 726, 729, 733
9140 726, 729, 733
9216 726, 729, 733, 857
9506 727, 729, 733
9509 727, 729, 733, 765, 857
9513 727, 729

A
AAA 33, 146–147
AAA Tab 146
access 392, 394, 396–397, 399–402, 412, 416, 430–431, 433–434, 436, 438, 445, 455, 473, 481, 503
access control 402–403, 555, 560, 571, 732–733, 755, 800, 811
access level 140
access limitation 39
activate 389, 450, 472, 478, 485–486, 492, 502, 508, 515, 539, 546, 550, 576
activate the zone set 546, 550
activation 386, 389, 394, 449–450, 466–467, 493, 535, 546–548, 554–555, 801, 814, 816, 836
active card 490
active configuration 223, 291, 323, 934
active CP 49–50, 56–57, 60–61, 102
active CP blade 49–50, 52, 56
active mode 869
active ports 790, 792
active zoning configuration 549
activity monitoring 143
add members 542, 545
adding
  end-to-end monitors 173
  filter-based monitors 178–179
Address Properties 455
addresses assigned 42
adjacent ISLs 10
Admin access level 140
Admin button 115, 272, 292
admin login 52
administration 7, 13, 25, 28, 34–36, 115–116, 798, 802
Administration tools window 116
administrative privileges 134, 292
administrator 756, 781, 784, 934
Advanced Performance Monitoring 7, 13–14, 163, 165, 172
Advanced Security 35, 38, 232, 274–276, 286–287
aggregate bandwidth 311, 827
AL_PA 29, 31, 37, 143, 153
AL_PA Level Zoning 294
AL_PA monitoring 163, 172–173
Alarm 182, 185
Alarm Notifications tab, Fabric Watch View 182
alerts 28–29, 247, 398, 401, 403, 440, 492, 507, 555, 560, 586, 592
Alias 79
alias 10, 79, 179, 221, 293, 295, 297, 797–799, 802–803
alias member 805–806
alias names 797
Alias tab 295, 297
alias wizard 79
aliases 94, 180, 222, 291–292, 294, 299, 303
allowable distance 315
analysis tools 854
analyzers 868
ANSI-based 401
Apache 32
API 40, 275
API server 143
APM 7
Application Specific Integrated Circuit 9
Arbitrated Loop 8, 143
arbitrated loop 523–524
Arbitrated Loop Physical Address 37
area 8, 30, 52, 87, 116
areas 29–30, 33, 39, 116, 786
AS 3, 5, 7, 9–10, 274
ASIC 9–10, 12–14, 19, 23, 509, 531

© Copyright IBM Corp. 1999-2007. All rights reserved.

ASIC interrupts 10
Assigning ports 787, 791
Atlas ASIC 509
ATM gateways 142
Attachment Reason Code 562
attention 401, 463, 496, 564, 576, 593
attention icon 526
attention indicator 593–595
attention indicators 403, 555, 560
audit 332
Audit log 588, 592
authenticate 743, 780–781
authentication 8, 28, 32, 38, 40, 732–733, 748, 755, 780–781
authentication traps 123
authority 433, 437–438
Authorization 774, 780–781
Auto 736, 759, 875
auto-configure 524
auto-negotiating 388–389
AutoNotify 878
auto-sensing 9, 388
auto-sensing capability 8
Auto-sensing speed negotiation 9
availability 399, 406, 496, 511, 516, 531, 573
Available Addresses 456
average data rates 391

B

B_Port 735
back pressure event 576–577
backup 39, 147, 227, 230, 275–276, 736, 761
backup configuration 481
backup copy 935
backup CTP 488, 490
backup FCS 39
balancing 18–19, 311–312
bandwidth 8, 11, 17, 19, 311, 391, 573
bar charts 580
baseline 224–226, 229–230
baseline file 229
basic management functions 1
basic monitoring 156, 158–159, 161
basic processor memories 12
basic setup functions 42
basic support software 16
basic zoning 69
BB 142
BB Credit 142
BB credit 928
BB Credits 509
BB_Credit threshold 575
BB_Credits 482, 509, 577–578
BE data processor 334
BE processor 334
beaconing 151, 603–605
Behavior Control 341
binding 387–388, 393, 402–404, 482, 534, 555–556, 733–734
binding features 403, 555
binding rules 561
blades 521
blinking 594
block ports 392
blocked 482, 508, 515, 532, 561, 938
bootflash 730, 736–737, 760–763, 765, 768–769, 774, 776, 778, 780
bootflash synchronization 771
bridge 735
broadcast 10, 290
broadcast frames 535
browser, Web 28, 87, 196, 272
buffer credits 929
Buffer limited ports 23
Buffer management 23
buffer reconfiguration 316
buffering 316
buffers 21–22, 37, 120, 142
buffer-to-buffer 142, 875, 928
buffer-to-buffer credits 578
business continuity 3, 5

C

cable lengths 17
cable wrap test 603
call home 237, 240, 242, 419–420, 507–508, 878
canvas 153–157, 159–160, 162, 164
Canvas Configuration List 156
canvas configurations 155
capture filters 869
cards 488, 510–511, 521–522, 573
cascaded directors 340
cascading 888
certificates 8, 38, 40, 276, 281
CFS 794
Challenge-Handshake Authentication Protocol 8,

40
Change Management Wizard 243, 245
Change Speed 150
change the domain ID 497, 903
CHAP 404, 732–733, 755
chassis wide 113
CIM 400
Cisco 725–726, 729, 731–733, 736, 738, 746, 755, 826, 890, 897
Cisco Fabric Analyzer 868
Cisco Fabric Manager 725–727, 730–732, 738, 740
Cisco Fabric Services 794, 878
Cisco MDS 9000 725–726, 730–731, 733–735, 737–740, 754–756, 758, 780–781, 794, 797–798, 818, 826, 829, 837, 849, 868–870
Claim Certificate 774
class F interswitch frames 142
Class of Service 95
classes 29–30, 181–182, 184–185, 187
clearing
    end-to-end monitor counters 178
CLI 387, 394, 399–400, 406, 430, 432, 463, 506, 520, 555, 598, 605, 730–731, 736, 738–739, 931, 934
CLI parser 731
Client 725, 731, 868–869
client logins 433
client sessions 434, 436
clock 934
command 20–22, 24–25
command line interface 12, 44, 115
command Modes 739
Common Information Model 400
communication 755–757, 786, 838, 938
community names 400, 482
community string 122–123, 406, 502–505
community strings 503
compare 855, 857
comparison report 229
compatibility 218
compatibility checks 771
concurrent 478
Condor 9, 13–14, 23
Config mode 740, 819
config mode 739, 819
configuration download 229
Configuration editor 164
configuration file 144, 219, 225, 227–228, 294, 729, 855, 897, 932, 935–937
configuration files 429–431
Configuration Manager 398
configuration mode 739, 794
configuration options 524, 555, 565
configuration parameters 41, 223–224, 228
configuration procedure 49
configuration task 438
configure ports 316
Configure Thresholds tab, Fabric Watch View 188
conflicts 218, 220–222, 304, 321–322, 324
congested links 391
congestion 11, 16, 143
congestion event 576
congestion thresholds 575
Connecting fiber optics 509
connection 21, 38, 40
Connectivity 737, 758, 854, 860–861
connectivity 737, 854, 860–862, 864, 868
consistent 496
console port 49
console serial port 757
control 398, 402–403, 405, 438, 482, 508, 531, 555, 560, 571
Control Device 341
copy 730, 736–739, 870, 934–936
Copy Configuration 746
copy processes 746
copying the firmware 488
core PID 54–55, 220, 273, 310, 325
Core PID format 54–55, 321
correct device 603
cost 18, 34, 327–328
cost value 328
counter values 177
counters 7, 28–29, 174, 176–178
CRC error measurement 163
CRC errors 30–31, 38, 163, 173
Create VSAN 786, 788
credits 21, 23, 317
cross-over cable 442, 446, 448, 451
cryptographic 404
CSR 280–282
CSRs 280–281
CTP 481, 486, 488–490
CTP switchover 489
cumulative counters 176
CUP 5, 14, 150, 340, 342, 388, 401, 580
CUP Port Connectivity 342

Current 7, 9–10, 13, 17
Current Speed 150
custom filter 179
cut-through 14

D

daemon 731, 868–869
data collection 596
data collection engine 331
data field size 142
data flow 391, 576
data frame path 24
data packets 311–312
data traffic 309, 868, 870, 875
date 745–746, 784–785
DCC 38, 41, 275
default cost 328
default IP address 44
default policy 19, 287
default VSAN 786, 793
default zone 392–393, 405, 482, 496, 534–537, 539, 554, 759, 786, 798, 808, 819, 897, 900
default zone policy 798, 898
defect call 594
degraded 592, 595
deleting
  end-to-end monitors 177
  filter-based monitors 181
denied access 559
deny 403, 555, 560, 563
destination domain 326–327
device 309
Device Connection Control 38, 41, 275
Device Connectivity Troubleshooting Wizard 249
device level zoning 10
Device Manager 731, 738, 740, 747–749
device performance 163
device selection panel 70
Device-based routing 19–20
DH-CHAP 8, 40, 404
DHCP server 407
diagnose 24
diagnostic checks 33
diagnostic commands 12
Diagnostics 12, 16, 33, 41
diagnostics 12
Diagnostics Test 599
DID 18–19, 21, 31, 38, 153, 164, 166–168
Diffie Hellman Challenge Handshake Authentication Protocol 755
Diffie-Hellman 8, 40
Diffie-Hellman Challenge Handshake Authentication Protocol 404
digital certificate 40
digital certificates 8, 28, 38, 40, 276, 282, 284, 286
director 343, 379, 386, 389–391, 394, 398–400, 403–404, 406, 452, 458–459, 478, 481–482, 488–491, 607, 725, 727, 742, 754, 762, 766, 879
director configuration 52
disable 757, 780, 794, 849
Disable Device Probing 142
displaying
  filter-based monitors 180
disruption 12, 16–17, 54, 275
disruptive 463, 466, 493, 915
distance 13, 17, 21–23
distances 578
DLS 326
DNS 515, 756, 759, 823
DNS host name 516
domain 14, 30, 42, 45, 50, 53, 77, 391, 393, 403, 482, 495–496, 498, 533, 579, 759, 788–789, 797, 830, 838
domain address manager 495
Domain ID 45, 53, 117
domain ID 30, 42, 45, 53, 93, 116–117, 143, 174, 391, 398, 403, 482, 496–499, 538, 555, 559, 575, 579, 786, 789, 797, 834, 862, 884, 890, 897, 903–904, 906
Domain ID configuration 903
domain RSCNs 393
download 421–423, 472, 476, 478–479, 481–482, 485–488
Download Firmware 122, 256
download protocol 214
download switch configuration 224
DPS 18–19
DPVM 793–795
DPVM configurations 793
duplex access 430–431, 433
duplicate alias names 221
Duplicate domain IDs 322
duplicate domains 322
Dynamic Load Sharing 325–326
Dynamic Path Selection 18
Dynamic VSANs 793

E
E/OSc 386
E_D_TOV 142, 482, 496, 579
E_Port 13, 23, 311, 524, 561, 572, 592, 735–736, 786, 818, 822, 825–827, 837–838, 873, 892–893, 928
E_Ports 30, 38, 309, 312, 316
ECCAPI port 432
ECHO 862
Edge 830
edge 829
EE mask 175
EEPROM test 12
EFCM 386, 391, 394, 396–401
EFCM Basic 386, 394, 404, 406, 446, 451, 463, 467, 478, 520, 568
EFCM logs 587, 590
EFCM server 386, 394–396, 398, 400–402, 406, 408, 412–414, 416, 418
egress 870, 872, 874
Egress source 873
EISL 735, 827, 875
EISLs 827, 837
element 343, 607, 879
Element Manager 386, 391, 396, 398, 400–401, 405, 438, 460, 463–464, 478–481, 483, 487–488
Element Manager logs 590–591
Elements 202–203
elements 7, 28–29, 182, 202, 797
ELP 310, 838
ELS 24
E-mail 397, 399, 401, 440–441, 507, 774, 878, 889
E-mail addresses 241
E-mail alerts 440, 492, 507
E-mail Configuration 182, 193
E-mail notification 243
Embedded Port 393, 591–592
Embedded port log 592
Enable Config 305, 308
Enabling DPVM 794
Enabling iSCSI 849
encoding method 389
encrypted 430
encryption 28, 431–432
end-to-end monitor 175–177
End-to-end monitoring 38, 163–164, 172–173
end-to-end monitors
  adding 173
  clearing counters 178
  deleting 177
  setting a mask 174–175, 178
enforce 8, 327
enforcement mode 404, 561, 566
enforcement mode configuration 565
enforcement modes 561
Enterprise Fabric Connectivity Manager 386, 395
ENTERPRISE_PKG 732, 829
Environmental classes 184
equal-cost paths 18
equivalent paths 326
error 343, 607, 879, 914–915
Error Detect Time Out Value 142
error detect time-out value 496
error light 604
Error log 120, 186, 322–324, 338
error messages 51, 120, 742
errors 29–30, 37, 142, 160, 163, 858
Ethereal 868–869
Ethereal GUI 869
ethernet 28, 41, 45, 47, 742, 756, 826, 838, 842, 869
ethernet port 838
Event Log 562, 576, 589, 592, 604
Event log 562, 577, 594
Event Management 398
events 29, 34, 56, 87–89, 97, 124, 203
Excel reports 33
exchange based routing 20, 325
Exchange Link Parameters 310
EXEC mode 739
Exec mode 739, 818–819, 865
existence 794
Expansion Port 311
expansion port 735, 822
Export 35, 209, 231
export logical group 209
Extended 3, 5, 7, 13–14
Extended Fabric Activation 37
Extended Fabrics 5, 23, 37, 146, 310, 315–316
Extended Link Service 24
external security 8
EZSwitch 61
EZSwitchSetup 65, 85

F
F_Port 524, 735–736, 873, 928
fabric address notification 143

Fabric Binding 403, 482, 555–560, 888, 896–898, 903, 905–908
Fabric Binding activation 555–556, 559
Fabric Binding configuration 556, 904, 906
Fabric Configuration Analysis 854–857
Fabric Configuration Server 38–39, 275, 288
Fabric Configuration Servers 35
Fabric Events 29, 87–89, 204
fabric exploration 42
Fabric log 527, 589, 592
Fabric Login 42, 209–210, 230
Fabric Management Policy Set 275, 287
Fabric Manager 4, 7, 32–35, 40, 52, 122, 194, 196–198, 725–727, 730–732, 738, 740–746, 831, 855
Fabric Manager Client 731
Fabric Manager Reports 251
Fabric Manager Server 731, 751, 780
Fabric Membership List 403, 555–557, 559
Fabric Merge 218–219
fabric operating parameters 224
Fabric Operating System 7, 16
Fabric OS 7–8, 11, 13, 32, 34, 38, 120
Fabric OS Version 4.0 16, 298
fabric outage 273, 287
Fabric parameters 53, 55, 142, 226
Fabric Port Name 95
Fabric Port WWN 95
fabric rejected 532
fabric routing 326
fabric security 755
fabric start up 499
Fabric Watch 3–5, 7, 13–14, 28–29, 34, 89, 181
Fabric Watch View
  Alarm Notifications tab 182
  Configure Thresholds tab 188
fabric wide setting 287
fabric wide settings 32
fabric zoned 546
fabrics 754, 786, 925
failed fan 114
failed state 594
failover 56, 108–112
FAN 30, 33, 97–98, 113, 143
Fan button 113
fan button 113
fans 7, 28–29, 77
FC ID 734–735, 797–798, 802, 804, 932
FC Ping 854, 862–863
FC PortChannel 827
FC Traceroute 854, 864
FC Trunking 827
FC4 Type 95
FC-AL 388–389, 523–524, 735
FC-FC 579
FCIP 726–727, 732, 837–838, 901
FCIP interface 838, 840
FCIP profile 838–839
FCIP tunnel 841, 843–844
FCIP wizard 841
FCIP/iFCP 329
FCP 890, 931
FCPING 24
FCS 38–39, 275, 284, 286–288, 290
FCS switches 288–291
FC-SP 732–733, 755–756
FDMI host name 94
feature activation 466
Feature based licensing 731
feature key 389, 403, 459–462, 466, 469, 555
fencing 392
Fiber optic 513, 515, 603
Fibre Channel 379, 392–393, 466, 497, 592, 605, 725–727, 732, 734–735, 755, 786, 826–827, 837, 849, 860, 868–870, 873, 890, 930
Fibre Channel frame 18, 164, 178
Fibre Channel IDs 734
Fibre Channel interface 870
Fibre Channel Line Card 827
Fibre Channel Port address 93
Fibre Channel Shortest Path First 311
FICON 4–5, 14, 19, 21, 388, 579, 726–727, 732
FICON cascaded 891, 903, 926
FICON CUP 14, 150, 340
FICON intermix 340
FICON IOCP 511
FICON management server 394, 401, 580
FICON Manager Server 340
filter 10, 29, 31, 164, 176, 178, 874
filter type 188
Filter-based monitoring 38, 163–164, 172, 178
filter-based monitors 178, 180–181
  adding 178–179
  deleting 181
  displaying 180
filtering 874
filters 869, 874
firewall 412, 416, 418, 428–431, 433, 448

firewall restrictions 869
firmware 1, 16, 33, 56, 77, 87, 97, 122, 201, 203, 214, 254, 754
firmware download 210, 214, 255–256, 263, 272–274
firmware image file 482, 484
firmware level 257
firmware levels 386, 390, 394
firmware library 398–399, 482–485, 488
firmware library database 484
firmware repository 32, 234–235
Firmware Tab 122, 272
Firmware upgrade 394, 488
firmware upgrade 214, 234, 272–273
firmware upgrades 386, 478
firmware versions 478
Fixed Zoning 69, 71, 78, 85
FL_Port 735–736
FL_Ports 873
flag 513–514
flag style 513
Flash Files 776
flexibility 533
FlexPorts 389
FLOGI 16, 30, 42, 793, 929
flow 10, 21, 46, 49
flow control 757
flow level 392
FM Ping 863
FML 403, 555
FMPS 275, 287
FMS 340, 401
FMSERVER_PKG 732, 751
FOS 7, 9, 12–13, 16, 20
frame 8, 10–11, 17–18, 312
frame buffers 317
frame data 391
frame decoding 868
Frame Distribution 17
frame filtering 8, 10
frame level 392, 531
frame routing priority 142
frame traffic 12, 171
frames 14, 18, 21, 38, 173, 798, 827, 837, 868–870, 875, 928
frames received 160, 328
frames transmitted 174–175
FSPF 311, 327, 339, 392
FSPF Route 327
FSPF routing table 328
FTP 32, 214, 234, 237
FTP server 32–33, 219, 225, 234, 272, 338–339, 736, 760–761, 768
FTP service 234
full bandwidth 11
Full Volatility 388, 391
fWWN 797, 928
FX_Port 735
Fx_Port 524

G

G_Port 524
gateway 756, 758–759
gateway manufacturers 310
GigE interface 838–839
GoldenEye 9, 13, 23
grace period 464
graph 153–154, 156, 160–161
graphical presentation 731, 744, 749, 825
graphing 153
graphs 153–154, 156–158
group 10–11, 17, 19, 22
Group log 589
Gx_Port 524

H

hacking 403, 555
Hard Address 95
hard zoning 798
Hardware 765, 782, 866
hardware 343, 607, 731–733, 737, 740, 760, 798, 879, 889
Hardware log 592
hardware symptoms 593
hash 404
Hayes-compatible modem 56
HBA port 69
health 33, 104, 113, 191, 854–855
health status 248
High Availability 4–5, 56, 108–109, 827, 909, 911
High Availability services 109
Historic 398, 581
historical performance 732
history log 592
hit count 164, 178
hop count 92, 327, 572
host ID 773

HotCAT 386
hot-swappable 388
HTTPS 8
HyperTerminal 400, 442–443, 445, 757

I

IBM default settings 190
identify 343, 607, 879, 897
iFCP 579
Images 768
images 729–730, 736–737, 763, 768
implementation process 754
Import 35, 209, 235–236
inconsistencies 219
increased link transmission 578
infrastructure simplification 3, 5
ingress 870, 872–874
Ingress source 873
initial configuration 416–417
initial server configuration 416
initialization 10, 21, 28, 42, 45–46, 735–736, 838
Initiate failover 109
initiators 829
in-order delivery 12, 18–19, 21, 38, 311–312, 327, 890, 897, 900
Insistent domain 498, 579
insistent domain ID 555
Install all 737, 762, 764
install options 742
installer 743, 752
installing performance monitoring 164
inter switch link 822
inter switch links 524, 837
Inter VSAN Path 830
Inter VSAN Routing 829
Inter VSAN Zone 829
Inter VSAN Zone Sets 829
interactive port card view 521
interconnected fabric 316
inter-mix 579
internal buffering 316
internal log 120
Internet Explorer 738
Interop Mode 495–496, 534, 579, 821
interop properties 788
interoperability mode 786
Inter-Switch Link 320, 572
interval number 177
introduction 380, 409, 424
intuitive 28
Invalid CRCs 30, 187
Invalid Words 30, 187
inventory messages 878
IOD 327
IP address 741, 747, 751, 756, 758–759, 797, 823, 838, 895, 918
IP services 837
IP storage 737, 837, 839
IP traffic 171–172, 178
IP versus SCSI traffic 164, 178
IPS module 731, 837, 849
iSCSI 579, 726–727, 732–733, 837, 849–850, 852–853
iSCSI initiator 849, 851
iSCSI wizard 850
ISL 4–5, 10–13, 17, 19, 37, 45, 92, 223, 243, 309, 311, 320, 388, 391–392, 524–527, 561, 572, 575, 735, 818, 822, 825, 827, 837, 843, 854, 894, 901, 908–909, 911–912, 915, 918
ISL R_RDY Mode 310
ISL Trunking 10–11, 13, 17–19, 38, 311–313
ISL trunking 38, 311, 313
ISLs 389–392, 496, 511, 573–574, 578
isolated 786, 794, 931
isolated VSAN 786
Issues 777, 829, 858, 862
IVR 732, 829–832, 834
IVR definitions 829
IVR NAT 831, 834
IVR Wizard 831

J

Java 731, 738, 740, 742
Java based 386
Java Runtime Environment 446
Java Web Start 731, 738, 742
JRE 446

K

key installation 462–463
Key recovery 461
kickstart 729–730, 736–738, 760–761
kickstart image 729–730, 737, 760, 765
kilometres 578

L
L10 653
labelling 513–514, 603
labelling machines 514
laser detection card 605
latency 19, 837
LD mode 21, 23
LD port 21
libpcap 868
library 394, 398–399, 472–473, 482–485, 488, 544
license 13, 32, 36, 731–733, 739, 760
license agreement 413
license file 230
license file installation 779
license key 133–134, 158, 164, 274, 276, 311, 313, 396, 415, 463, 773–774, 889
license keys 16, 126
licensed 391, 398, 460, 462–464, 566–567, 576, 581
Licensed Port 149
licenses 733, 739, 760, 765, 773
Licensing 7, 36, 230–231
licensing 7, 230, 282, 387, 458, 463–464, 467, 731, 733, 775
licensing information 230–231
licensing options 36
light 604–605
lighthouse icon 151
limited ports 23
limits 390, 534
link 735, 786, 822, 827
link cost 328–329
Link incident log 592
Link Loss 30, 187
link speed 9
Linux 3, 16, 120, 731, 740, 868
load balancing 19, 311–312, 786, 788, 890, 897, 901, 908
load sharing 325–326
load-balancing 18
loader 729, 760, 762–763, 765
local files 35
locked 559, 935–936
log 895, 898
log file 877
logged in devices 796
logging events 56
logical groups 35, 205, 209
logical interface 826, 908
logical ISL 10–11
logical partitions 528
logical switch 50, 121, 144
login 739, 748, 753, 758
login credentials 743, 752, 768, 777
logs 393, 397–398, 401, 523, 527, 577, 586, 590
Long Distance 23
long distance 21, 23, 315–317
long distance levels 316
loop 735
loop configuration 163
loop devices 523, 734
loop initialization 143
loop test 603
loop-back function 13
lower provisioning time 12
lowest cost path 328
LPAR 392
LSAN 33, 251
LUN level zoning 10
LUN masking 537, 821
LUN per 169–171
LUN zoning 821
LUNs 537
LUN-zoning 733

M
M12 9, 16–17, 39
M12 zoning 298
M14 4, 9, 16–17
MAC 38–39, 275
Main view 97
MAINFRAME_PKG 732
maintenance 399–400, 402, 438, 442, 468, 481, 483, 493, 507–508, 592, 596
maintenance port 394, 400–401, 442–443, 445–446
maintenance window 478
manage licenses 230
manage multiple fabrics 32
management xiv, 379–380, 386, 391, 394–395, 397–398, 400, 729–733, 738–739, 797, 838, 888
Management Access Control 38–39, 275
management ethernet 756
management functions 1, 7, 28, 34
Management Information Base 31
Management Tools 730, 740
Management tools 7, 52, 738

management tools 386
manual installation 738
manual intervention 398, 559
mapping information 793
mappings 734
mask 44, 48, 66, 120–121, 174, 756, 797
mask for end-to-end monitors
  setting 174–175, 178
master DPVM switch 796
Master log 590
masterless trunking 16–17
McDATA File Center 473
mcdataClientInstall.exe 423
MDS 9000 725–726, 729–731, 733–735, 737–740, 754–756, 758, 780–781, 786, 794, 797–798, 818, 826, 829, 837, 849, 868–870
MDS 9216 756–757
MDS 9506 756
MDS 9509 756
member 390–391, 531, 533–534, 542, 545, 560
membership 787–788, 793–794, 805
Membership List 403, 555–557, 559–560
memory 740, 765
merge 579, 819, 822–824
merge analysis 822, 824
Merge manager 220, 222
merging 218, 223, 320
merging two fabrics 322
message integrity 28
metric 327
MIB 31
microcode levels 255
Mixed Level Zoning 293
mixed zoning scheme 293
mixing switch types 21
Mode 735–736, 739, 759, 786–787, 794, 818–819, 821, 828–829, 838, 870, 875
modem 396, 400, 419, 442–443, 446
modem connection 56, 60
modem lamps 60–61
modem serial ports 56
Modem Setup 56, 59
Modifying zone 550
monitor 8, 10, 28–29, 31–32, 35, 51, 162, 814, 854, 870, 874, 877–878
monitor elements 29
monitor LEDs 97
monitored 740, 871, 874
monitored element 29
monitoring 390, 392, 398, 401, 580–581, 584, 730, 732, 735, 870, 874, 877
monitoring service 247
monitoring switch activity 140
monitors 28–30, 34, 163
MTU 928
multicast 10
multi-link trunks 17
Multiple switch environment 822
multiple zone sets 801
multiplex 735, 786, 826
multiswitch environment 145, 201
multiswitch fabric 495

N
N_Ports 734
name server 10, 88, 92–93, 96, 798, 930
Name server enforced zoning 531
name server entries 92
name server information 930
Name Server table 92, 94–96
names 797, 829, 897, 932
Navigation Tree 202–203, 207, 209
Netscape 738
Network Access Server 146
Network Config 119–121
network settings 121
network-admin 781, 784
network-operator 781–782, 784
new alias 295, 297, 301
new fiber 603
new messages 120
new password 65, 139, 289
new zone 535, 540, 544, 547, 807–808, 811, 813, 817
new zone set 544
nickname 399, 492, 516–520, 526, 533, 538, 542
nicknames 397, 514–516, 518–520, 526, 533, 542
NL_Ports 734
node symbols 537
node World Wide Name 793
non-disruptive 463, 466
non-disruptive failover 109, 111
Non-FCS 39, 289–290
non-intrusive 870
nonvolatile storage 301
null modem cable 446
numbering scheme 14–15, 510–511, 513

NVRM log 877
nWWN 793

O
one power supply 190–191, 193
online 403, 466, 493, 508, 560–562, 564
open fabric management 7
Open Fabric mode 496
Open Systems 890, 925, 931
Open Systems Management Server 401, 506
Open Trunking 388, 391–393, 460, 575–576, 591
Open Trunking log 577, 592
operating parameters conflict 324
Operating system 729, 739–740, 760, 765
operational modes 735
Operator 343, 607, 879
optic monitoring 390
optimal throughput 392
optional features 379, 397, 401–402, 458, 468
Options policy 275
organizational tree 182–183, 188
OS 386, 388, 390–392, 394, 400–401, 472
OSMS 394, 401, 460, 506
overlap 322
overlapping zones 390
overwrite 820
OXID 18, 21

P
packets 745
paddles 511, 530
PAK 774, 780
parameters 756–757, 829, 838, 874
part number 594
partition 528–530
partitioning 528
Passive mode 869
password 47, 50, 52, 60, 65
passwords 8, 32, 38, 40, 50, 232, 289
Pay on Demand 13
peer IP address 838
perfAddEEMonitor command 173
perfAddIPMonitor command 178
perfDelEEMonitor command 177
perfDelFilterMonitor command 181
performance 1–2, 5, 8, 10, 29, 398–399, 404, 406, 431, 511, 573, 578, 580–581, 583–586, 731–732, 740, 751–753, 854, 908
Performance Bundle 13, 311–312
performance graph 153
Performance Graphs 158, 161, 164, 166
performance management 163
Performance Manager 731, 751–753
Performance Monitor 29, 31, 152–154, 156, 182, 188
Performance Monitoring 580
performance monitoring 4–5, 7, 10, 13–14, 37, 154, 163–164, 166, 172, 398, 580, 584
perfSetPortEEMask command 174–175, 178
perfShowFilterMonitor command 180
permissions 755, 781, 784
permit 403, 555, 560, 563
Persist Fabric 525–526
Persist fabric 525, 589
Persisted Fabric 525–526, 589
persistent 25, 149–150, 164, 734–735, 801, 932
Persistent FCIDs 734, 890
Persistent FcIds 734
PFE 458
physical access 8, 40
physical inventory 33
ping 854, 860, 862–863
PKI 8, 40, 278
PKI Cert utility 280
PKICert 280, 282–283
PKICert utility 279, 283–284
Planning Manager 398
PLOGI 532, 862
POD 13, 36
policies 392
policy basis 35
port area number 298–299
Port Binding 403, 534, 560, 562, 566–567
port blades 14, 49, 102
port characteristics 444
port configuration 398, 482, 508, 524, 931–932, 934, 938–939
port count 510, 573
port diagnostics 598–602
port failure 533
port filter statistics 164, 178
Port Groups 206–207, 312
port information 99, 102, 928
Port IP Address 95
port layout 509–512
port level zoning 10
Port Login 862

port matrix 317
port modes 734–735
Port Name 95, 150
Port number 93, 149, 153, 161, 167, 170
port numbering 881
port numbers 534
port position 92
port properties 757
Port RSCN Suppression 25
Port security 732, 755
Port Selection 167, 170
Port State 97, 149–150
port states 105
port syslog messages 878
port throughput capability 13
port values 431
Port VSAN membership 793
port zoning 496
PortChannel 822, 826–827, 829, 845, 848, 873–874, 908–909, 911–913, 916, 926
Ports On Demand 3, 7, 13, 36
Ports tab 147, 149
Poseidon ASIC 509
POST 12, 41–42, 49, 60
power 343, 607, 879
Power On Sequence 41
power redundancy 595
power supplies 3, 7, 14, 29, 77, 193, 389, 528, 530
power supply 14, 33, 98, 113, 190
power-on self tests 12
preferred domain ID 482, 497
preferred port 524
pre-installation information 410, 425
Primary FCS 39, 287, 291
Primary FCS switch 39, 287
primary interface 407
principal switch 42, 386, 495–496, 598
problem description 594
problem determination 92, 605
problem results 855
problem with unapproved code 755
problems 855
Product Administrator 402, 438
Product Authorization Key 774
product feature enablement 458–459
product functions 396
Product status log 590
progress window 450
Proof of Purchase 774
proposed configuration 836
protection 380, 403, 555
Protocol Error 30, 187
protocol level zoning 10
Public Key Infrastructure 40
public loop 93, 143
PuTTY 290
pWWN 793, 797–801, 815–816

Q
quad 317
Quick Setup 61
quick upgrade 738
QuickLoop 30, 294, 297

R
R_A_TOV 142, 482, 496, 579
RADIUS 404, 572, 732–733, 755, 781
RADIUS authentication 146
RADIUS client 146
range monitoring 29
ranges 29, 142
rapid access 34
rapid parameter 143
RBAC 27
real-time alerts 29
real-time traffic monitoring 392
reboot 16, 25, 56, 122, 150, 209, 215–218, 230, 734
reboot group, click 216
Reboot groups 202, 206, 217
reboot groups 215
reboot switches 217
rebooted 36, 218, 230, 260, 273
reboots 734
recipient IP address 123
reconfigure WWN 533
Redbooks Web site 967
redundancy 573, 595, 908
Redundant power 388–389
registered product 474
Registered State Change Notifications 535
Remote Authentication Dial In User Service 404
Remote Capture Protocol 869
remote distribution 310
remote EFC Manager 406, 422
remote procedure calls 143
Remote Switch 310, 326

remove members 564
removing
  end-to-end monitors 177
  filter-based monitors 181
Replicate AAA Configurations 33
report window 116, 140, 145, 273
reports 405, 583–584
Request Certificates 282
request packet 745
requirements
  switch 5, 194
  workstation 195
resolutions 858, 860
Resolve Issues 858
Resource Allocation Time Out Value 142, 496
resource sharing 829
resources 343, 607, 879
response packet 745
restarts 164
Restrict All 404, 561, 566
restrict attachment 566
restrict connectivity 496
Restrict E_Ports 404, 561
Restrict F_Ports 404, 561
rights 397, 436, 438
RJ-45 756
RLS probing 143
RMON 878
role 27, 110, 141, 149
Role Based Access Control 27
role based authorization 780
roles 781–784, 868, 890
route 391, 572, 574, 605
Route table enforced zoning 531
route tables 390, 531
router 578–579
routes 11, 19, 327, 860, 865
Routing 10, 20, 142, 145, 173, 391, 531, 574, 578–579
routing 10, 14, 18–20, 142
routing database 392
Routing policies 20–21
routing tab 146, 325
routing table 42, 327–328
routing tables 10, 17, 42, 391, 909
RPC 143
RPCAP 869
RSCN 10, 25–26, 143, 393, 535
RSCN suppression 25
RSCNs 25–26, 393, 482
RSHD 214
RSPAN 870
rstatd 143
running configuration 736, 746, 761, 814, 934
running-config 736, 762, 801, 866
rusersd 143
rx 872, 875
RX Performance 30, 187
RX Power 31, 186

S
safe zoning mode 534
SAN data collection 33
SAN Director 4
SAN Health 329, 335
SAN Layout 334
SAN routers 579
SAN_EXTN_OVER_IP 732–733, 839
SAN140M port layout 510
SAN16B-2 3, 12–13
SAN256B 4–5, 12, 14–15, 46, 49–50, 56
SAN32B-2 3, 12, 46
SAN32M-2 port layout 509
SANavigator 397
SAN-OS 725, 729, 736–737, 739, 742, 760, 765–766, 774, 777, 793, 834, 864
SANpilot 386, 394
SANplicity Wizard 442, 446
SANtegrity Authentication 387–388, 404, 567, 569–572
SANtegrity Binding 387–388, 393, 403, 555–556, 561, 566
SANtegrity Fabric Binding 403, 555
SANtegrity Security Suite 397, 402
SANtegrity Switch Binding 403, 560
Save Config 302, 308
SCC 38, 40, 275
Scheduling 737
SCSI command graph 169
SCSI Enclosure Services 28
SCSI graph 169, 171
SCSI INQUIRY 93
SCSI read 21, 164, 169–170, 178
SCSI Read and Write commands 178
SCSI routing 849
SCSI traffic 163–164, 172, 178
SD port 876

SD_Port 735, 870, 872, 874–875
SDRAM 12
second CTP 488
secondary network interface 407
secrets 397, 404, 567
sectelnet 40, 286–287, 290
secTelnet client 40
secure channels 40
secure environment 288
secure fabric 1, 38, 40, 274, 277
Secure Fabric OS 8, 34, 38, 40, 274–275, 340
Secure HTTP 8
Secure Management Channels 38, 40
secure mode 40, 287
Secure Shell 40
Secure Socket Layer 8
Secure Sockets Layer 28
Secure Telnet 275, 285–287
Secure Telnet Client 284–285
secure Telnet session 286
Security 5, 7–8, 14, 27–28, 35, 38–39, 732–733, 755
security 5, 8, 33, 35, 38, 379–380, 387, 391–393, 397, 402–403, 405–406, 438, 502, 531, 534–535, 537, 555, 560, 567, 572, 587, 590–592, 903
Security Center 397, 405
security level 275
security policies 141, 232–233, 243, 287, 291
security policy check 248
security suite 733
segment 579
segmentation 30, 322, 324–325, 822
segmented 218, 322
separate fabrics 33, 251, 320, 322
Sequence Level Switching 142
Sequence Rebooting 215
serial cable 45–46, 48–50, 756
serial communication programs 46, 49, 59
serial connection 47, 49, 51–52
serial console 730, 738
serial number 396, 415, 458–462, 474, 594, 773–774
serial port 41, 46, 48–49
SerialLink 13
Server installation 399, 416
server requirement 396
server serial number 415
service call 594
Session log 590
setting mask for end-to-end monitors 174–175, 178
Setting up FCIP 838
settings 22–23, 32, 44–45, 53, 55
setup 3, 13, 21, 33, 41
setup program 756–757
SFOS 8, 38, 40, 274, 276
SFP 13, 30–31, 53, 929
SFP classes 185
SFP serial ID 118
sharing 8, 11, 19, 209
shipping plug 46, 48, 52–53
Show Tech Support 865–866
SID 18–19, 21, 31, 38, 164, 166–168
SID/DID 167–169, 188
SID/DID pair 153, 169, 174
SID/DID performance monitoring 166
Signal Loss 30, 187
Simple Network Management Protocol 7, 28, 31
simple network management protocol 400
single port access 431
single power supply 193
Single signon 32
slot number 298, 319, 734
slot/port 167, 170, 298–299
Slot/port method 298
slots 50, 102, 298, 319
SMART SFPs 29
SMC 38, 40
SMI-S 387, 394, 400
SML 561
snapshot 160, 180, 243
snapshots 246
SNIA 400
SNMP 7, 10, 28, 31, 40, 122–124, 224, 227, 387, 394, 397–398, 400–401, 405–406, 421, 455, 482, 502, 504–505, 576–577, 589–590, 730, 738, 740, 745, 756, 758, 782, 932, 935
SNMP information 224
SNMP parameters 122
SNMP protocol 745
SNMP settings 502, 505
SNMP timeout 745
SNMP trap 28–29, 186
SNMP traps 124
SNMPv1 trap 123
SNMPv3 730, 733, 755
SNMPv3 trap 123–124
SOF 180
soft zoning 798

software based 8
Solaris 731, 740
source files 754
source interface types 873
Space 737, 740, 761, 768–769
SPAN 870–871, 873–875, 909
Span Destination 735, 870
SPAN port 871
SPAN session 874
SPAN source 871
SPAN traffic 871
speed 9–10, 12, 14, 23, 30, 149, 388–389, 523, 798, 868, 875, 914
speeds 388
SSH 40, 275, 290, 730, 733, 738–739, 755, 759, 877
SSH client 290
SSL 8, 28, 430–432
Staged Port Bring Up 16
staged upgrade 264
standard filter-based monitors 178–179
standby CP 49, 57, 60–61
startup configuration 736, 739, 746, 761, 814, 818, 821, 836, 934
startup configuration file 729
startup-config 736, 801
state changes 29–30, 187
stateless protocol 745
static domain IDs 903
static domain ids 788–789
static label 514
Static Route 328
static routes 327–328
static zoning 533
statically allocated 403, 555
statistics 398, 580
statistics gathering 179
Status button 104, 113, 190
status notification 778
Storage Management Initiative Specification 400
Storage Networking Industry Association 400
summary information 32, 116
supervisor 729, 737, 765, 873
supervisor bootflash 761
supervisor module 756, 761, 868, 873
SupportSave 339
suppression 25
suspended 788, 794
switch
  requirements 5, 194
switch administration 140
switch agent 31
Switch Binding 403–404, 482, 560–567
Switch Binding Disablement 562
Switch Binding rules 561
Switch Binding violation 562
switch configuration 39, 122, 140, 224
Switch Connection Control 38, 40, 275
switch date 501
switch fabric 744, 746, 786, 860, 872–873
switch firmware 254
switch functionality 12, 310
Switch Groups 206
Switch Health 854
Switch Health Analysis 855
switch IPL 466
switch manager 68, 75
Switch Membership List 403, 560–566
switch name 45, 52, 68, 75, 87, 116–117, 756, 758
switch offline 493–494
switch operating parameters 495, 535
switch pair 842, 846
Switch PID Format 55, 142
switch port numbers 533
switch ports 403, 496, 499, 509, 560, 579–580, 592, 870, 928, 930
switch state 494
switch views 87
Switch/Port Level Zoning 294
SwitchAdmin access level 141
switchover 489–490
switch-to-switch authentication 8, 38, 40
symbolic name 149–150
Sync Loss 30, 187
syslogd 120–121, 306
system 725, 729–730, 735–740
system image 729–730, 736–737
system message logging 877
System Services 143

T

target switches 228–229
TE_Port 735, 825, 827, 873
TE_Ports 735–736, 786, 825–826, 837, 873–874, 928
Technical Assistance Center 878
Telnet 40, 49, 52, 54, 97, 107, 113, 325, 394, 399,

404, 430, 432, 506, 568, 730, 738–739, 759, 764, 877
Telnet CLI 605
telnet session 399
Temp button 114
Temperature 30, 114, 185–186
temperature 7, 29–30, 77, 97–98
temporary license 838
TERM 729, 826
terminal emulator application 45–47, 49–50, 59
test 441, 447–448, 598–602
TFTP server 730
third party management applications 32
Threshold 182, 184–185, 188, 193
threshold 17, 28–29, 38, 182, 185, 188, 190
Threshold alert 393, 591–592
thresholds 114, 182–188
throughput 8, 10, 13, 17, 28
throughput graph 160, 162
time 392, 416, 441, 458, 496, 499, 501–502, 515, 534–535, 555
timeout value 147, 258
TL_Ports 735, 873
toolset 730–732, 738
Topology 10, 23, 28, 53, 87–88
topology 537, 557, 793, 830
topology changes 327–328
topology reconfigurations 29
topology report 91–92
TotalStorage Storage Switch L10 654
Trace Dump 338
traceroute 854, 860, 864
traffic 392–394, 430–431, 433, 466, 508, 537
traffic flow 391
traffic load 10, 17
traffic type 870
transaction codes 458–459, 461–462
transaction performance 163
transfer protocol 777
Transit 830
transit 829
translative loop 735
transmitter negotiation 41
trap level 122–124
trap message recipients 400
tree structure 181
trigger value 28
tri-rate SFP 13
troubleshoot 586
troubleshooting 1, 24, 85, 163, 248–249, 329, 379–380, 586, 731, 798, 802, 865, 877
trunk group 17, 19
trunk master link 12
trunk setting 825
Trunking 4–5, 7, 10–11, 13, 16–18
trunking 10–14, 16–17, 19, 38, 149–150, 315, 786, 826–827, 838, 874, 894
trunking architecture 17
trunking E_Port 735, 826–827
trunking group 312
trunking groups 53, 312
trunking implementation 575
trunking master 312
trunking performance 163
trunking ports 312
Trunking Tab 150
Trunking Telnet commands 313
tuning 575, 577
tunnel 841, 843–844
two port 431
TX Performance 30, 187
TX Power 31, 186

U
under-utilized 391
unencrypted 430
unicast 10, 42
unique domain IDs 830, 834
unlicensed 200
unlicensed ports 23, 36
unused ports 508
upgrade 54, 85, 210, 214, 230, 737–738, 742–743, 760–762, 764
upgrade firmware 210
upgrades 386, 478
upgrading firmware 276
Upgrading SAN-OS 760
upload 122, 144–145, 224, 227, 230
UPM 510–511, 521
URL 774
User access level 140
user account 137–139, 402, 433
user accounts 402
User Administration 136
User authentication 755, 781
user interface 343, 607, 879
user rights 438

User tab 136
user-level password 445
users 396, 404, 436, 438, 441, 568, 590, 755, 780, 782–785, 935

V
variables 737–738, 763
VE_Port 837–838
VE_Ports 837
vendor company 94
verification 755, 794, 849
verified 562
virtual channels 142–143
Virtual Channels parameters 143
Virtualization 388, 392
virtualized 834
Visio 330, 334, 336
VLAN 870
Voltage 31, 186
VSAN 726–727, 732–735, 755, 759
VSAN membership 787, 793
VSAN trunking 827
VxWorks 16, 41

W
WAN gateway 310
warranty 474
Web browser 28, 87, 196, 272, 731, 738, 741, 747, 751
Web Tools 203
WEB TOOLS license 200
WebTools 3, 5, 7, 13–14, 22–23, 28
Wizard 411–412, 442, 446–451
wizard 731, 766, 768–769, 771
workload peaks 11
workstation
  requirements 195
world wide name zoning 10
wrap 513–514, 598–602
wrap plug 598, 600, 603
wrap style 513
WWN 17, 24, 39–40, 77, 390, 403, 495–496, 516, 519–520, 531, 533–534, 542, 555, 557, 559–562, 564, 566–567, 598, 605, 733–734, 755, 793, 797–798, 802, 928
WWN Level Zoning 294
WWNN 93
WWPN 92–93, 533
WWPNs 533, 542

X
XML file 231

Y
yellow triangle 526

Z
zip file 596
Zone Admin function 291
zone changes 29–30
Zone distribution 818
Zone limits 390
Zone management 534
Zone member definition 533
zone members 798, 801, 812, 816
zone merge manager 220
zone name 799–801, 815–816
zone set 392–393, 482, 534–535, 537, 540, 544, 800–803, 811
zone set database 815, 819–821
zone set distribution 819–821
zone sets 396, 398, 534–536, 539–540, 544, 550, 579, 800–801, 811, 815
zones 92, 94, 118, 291–292, 732, 786, 799–801, 807, 811, 819, 838
zoning 3, 5, 8, 10, 13, 379, 387, 390, 392–393, 398, 402, 405, 482, 498–499, 515, 531, 533–535, 537, 539–540, 549, 732–733, 797–798, 801–802, 816, 819, 831, 890, 897, 925
zoning configuration 25, 69, 223, 248, 303
Zoning Configuration Analyze 304
zoning dialog 539–540, 542, 544, 546
zoning example 536, 546
Zoning icon 96
zoning inconsistency 322
zoning information 223, 275, 321–324
zoning license 85, 292
zoning matrix 83
zoning mode 392, 534
zSeries 401, 511, 579–580

IBM System Storage: Implementing an IBM SAN

(1.5” spine)
1.5”<-> 1.998”
789 <->1051 pages

IBM System Storage: Implementing an IBM SAN

Discover the latest additions to the IBM SAN family

Enhance your skills while using an easy-to-follow format

Grow with the new technology

“Do everything that is necessary and absolutely nothing that is not.”

In this IBM Redbooks publication, which is an update and major revision of the previous version, we have tried to consolidate as much of the critical information as possible while covering procedures and tasks that are likely to be encountered on a daily basis.

Each of the products described has much, much more functionality than we could ever hope to cover in just one book. The IBM SAN portfolio is rich in quality products that bring a vast amount of technicality and vitality to the SAN world. Their inclusion and selection is based on a thorough understanding of the storage networking environment that positions IBM, and therefore its customers and partners, in an ideal position to take advantage by their deployment.

We cover the latest additions to the IBM SAN family, which includes products from companies such as Brocade, QLogic, Cisco, and McDATA. We show how they can be implemented in an open systems environment, we focus on the Fibre Channel protocol (FCP) environment in particular, and we have included a FICON quickstart section. We address some of the key concepts that they bring to the market, and in each case, we give you an overview of those functions that are essential to building a robust SAN environment.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-6116-06 ISBN 0738486256